UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007

Por:
Cristhian Yonatan Calisaya Sana,
Milton Tarrillo Villegas

Asesor:
Mg. Fernando Manual Asin Gomez

Lima, Marzo de 2018

Área temática: Ingeniería y Comunicaciones

Línea de Investigación – UPeU: Gestión de TI

Calisaya Sana, Cristhian Yonatan
Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007, 2018 / Cristhian Yonatan Calisaya Sana, Milton Tarrillo Villegas; Asesor: Mg. Fernando Manuel Asin Gomez. – Lima, 2018.
273 páginas: gráficos, tablas

Tesis (Licenciatura), Universidad Peruana Unión, Facultad de Ingeniería y Arquitectura
Escuela Profesional de Ingeniería de Sistemas, 2018
Incluye: referencias, resumen y anexos

1. Ley de Protección de Datos Personales 2. Medidas de Seguridad 3. Control de seguridad 4. NTP-ISO/IEC 17799:2007 Tarrillo Villegas, Milton, autor.

http://repositorio.upeu.edu.pe/handle/UPEU/1380

DECLARACION JURADA
DE AUTORÍA DEL INFORME DE TESIS

Fernando Manuel Asín Gomez, de la Facultad de Ingeniera y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que el presente informe de investigación titulado "Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007" constituye la memoria que presenta el Bachiller Cristhian Yonatan Calisaya Sana para aspirar al título de Profesional de Ingeniero de Sistemas, cuya tesis ha sido realizada en la universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente declaración en Lima a los 25 de Julio del año 2018

Fernando Manuel Asín Gomez

Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007

TESIS

Presentada para optar el título profesional de Ingeniero de Sistemas

JURADO CALIFICADOR

Dra. Erika Inés Acuña Salinas
Presidente

Ing. Lizeth Geanina Huanca López
Secretario

Mg. Sergio Omar Valladares Castillo
Vocal

Mg. Immer Elías Cuellar Rodríguez
Vocal

Mg. Fernando Asín Gomez
Asesor

Ñaña, Lima, 01 de marzo del 2018

AGRADECIMIENTOS

Gratitud por sobre todo a Dios, el artífice principal de esta investigación.

Gratitud a nuestros padres y familiares por su apoyo incondicional.

Gratitud a nuestra prestigiosa casa de estudios la Universidad Peruana Unión y a sus colaboradores por permitirnos desarrollar nuestra investigación en sus centros de trabajo.

Gratitud a los profesionales que contribuyeron con su conocimiento y experiencia a la investigación, y de una manera particular a nuestro asesor él Mg. Fernando Asín Gómez.

Índice de contenido

Índice de figuras

Índice de tablas

Índice de anexos

Lista de acrónimos

ANPDP: Autoridad Nacional de Protección de Datos Personales.

BDP: Banco de Dato Personal.

DIGETI: Dirección General de Tecnologías de Información.

IEC: International Electrotechnical Commission (Comisión electrotécnica Internacional).

ISO: International Organization for Standardization (Organización Internacional de Normalización).

LPDP: Ley de Protección de Datos Personales.

MOF: Manual de Organización y Funciones.

NTP: Norma Técnica Peruana.

PDCA: Planificar, Hacer, Verificar y Actuar.

SG: Secretaría General.

TIC: Tecnologías de la Información y la Comunicación.

UPeU: Universidad Peruana Unión.

Lista de definiciones

Banco de datos físico: Es un conjunto de datos personales no automatizado.

Banco de datos lógico: Es un conjunto de datos personales en soporte automatizado.

Confidencialidad: Es el aseguramiento del acceso a documentos solo por personas autorizadas.

Controles/Control: Es un mecanismo utilizado para asegurar un determinado servicio y/o activo. Los controles pueden ser procedimientos, formatos, tecnología, etc.

Datos personales: Es aquella información que hace identificable a toda persona natural como: nombres, dirección, sexo, edad, etc.

Disponibilidad: Es el aseguramiento de la información y/o servicio a las personas que lo requieran en todo momento.

Documento inválido: Es un documento obsoleto, no utilizable o innecesario, potencialmente a ser eliminado**.**

Información: Es la interpretación que se le da a un conjunto de datos, puede estar de manera física como lógica.

Integridad: Es el aseguramiento de información exacta, verídica y completa.

Matriz RACI: Matriz de Asignación de Responsabilidades.

Política específica: Es una guía con un nivel menor, determina ciertos procesos y es delimitado por su alcance.

Política general: Es una guía a nivel de aplicación general, su impacto es alto y crítico.

Política: Es una guía orientada a la acción que debe ser divulgada, entendida y acatada por los miembros de una organización o área (siendo el caso de la investigación).

Procedimiento: Es un modelo de conjunto de acciones que debe realizarse para lograr un objetivo.

Recuperación: Es la acción de poner en disponibilidad al respaldo realizado con anterioridad.

Respaldo: Es la acción de realizar una copia a la información independientemente del tipo de respaldo que se realice (parcial o total).

Securizar: Realizar cambios y/o actualizaciones en los sistemas informáticos con el fin de lograr un alto nivel de seguridad ante ataques internos o externos.

Tratamiento de datos personales: Es cualquier operación que permite la recolección, conservación, modificación o eliminación de datos personales.

Trazabilidad: Es la capacidad de registro de las operaciones y/o actividades realizadas desde su origen hasta su destino.

Resumen

Actualmente las organizaciones invierten fuertemente en securizar sus sistemas informáticos, concientizar a sus colaboradores y contratar consultorías para el cumplimiento de normas internacionales y leyes relacionadas a la seguridad y privacidad; esto se debe a raíz de: ataques cibernéticos, robo de información, daño de imagen institucional, altas multas por incumplimiento de la legislación y otros riesgos relacionados.

En el Perú la Ley de Protección de Datos Personales (LPDP) es obligatorio para todas las organizaciones que traten con datos personales, las sanciones por incumplimiento vienen a ser de 0,5 Unidades Impositivas Tributarias (UIT) hasta 100 UIT.

La presente investigación se enfocó en el Capítulo V "Medidas de Seguridad" del Reglamento de la LPDP en las áreas de Dirección General de Tecnología de Información (DIGETI) y Secretaría General (SG) de la UPeU, por lo tanto, se implementó controles de seguridad basados en la NTP-ISO/IEC 17799:2007, un código de buenas prácticas para la gestión de la seguridad de la información en una organización.

La metodología para el desarrollo del proyecto contempló las siguientes etapas: En primer lugar, se llevó a cabo la Etapa 1– Auditoría preliminar; a continuación, se realizó la Etapa 2-Planificar la mejora en base a los controles de la NTP-ISO/IEC 17799:2007; después la Etapa 3-Ejecutar controles para la mejora de "Medidas de Seguridad"; posteriormente la Etapa 4-Evaluar y comparar resultados; por último, la Etapa 5-Determinar el nivel de mejora.

Como resultado de la investigación se logró implementar controles de seguridad, y así mejorar el nivel de cumplimiento del Capítulo V "Medidas de Seguridad" del

Reglamento de la LPDP en el área de DIGETI y SG de la UPeU; promover una cultura de seguridad de la información e impulsar el cumplimiento de la LPDP a nivel corporativo.

Palabras clave: Ley de Protección de Datos Personales, Medidas de Seguridad, Control de seguridad, Tratamiento físico, Tratamiento lógico, NTP-ISO/IEC 17799:2007.

Abstract

Currently, organizations invest heavily in securing their computer systems, raising awareness among their collaborators and hiring consultants to comply with international standards and security related to security and privacy; this is due to the root of: cyber attacks, information theft, institutional image damage, high fines for non-compliance with legislation and other related risks.

The present investigation focused on Chapter V "Security Measures" of the Regulations of the LPDP in the areas of General Directorate of Information Technology (DIGETI) and General Secretary (SG) of UPeU, therefore, controls were implemented of security based on the NTP-ISO / IEC 17799: 2007, a code of good practices for the management of the security of the information in an organization.

The methodology for the development of the project, contemplated the following stages: In the first place the Stage 1- Preliminary audit was carried out; then Stage 2-Plan the improvement based on the controls of the NTP-ISO / IEC 17799: 2007; then Stage 3-Execute controls for the improvement of "Security Measures"; then Stage 4-Evaluate and compare results; Finally, Stage 5-Determine the level of improvement.

As a result of the investigation, it was possible to implement security controls, and thus improve the compliance level of Chapter V "Security Measures" of the Regulations of the LPDP in the area of DIGETI and SG of UPeU; promote a culture of information security and promote compliance with the LPDP at the corporate level.

Keywords: Personal Data Protection Law, Security Measures, Security Control, Physical Treatment,Logical Treatment, NTP-ISO / IEC 17799: 2007.

CAPÍTULO I: GENERALIDADES DE LA INVESTIGACIÓN

1.1 Título de la investigación

Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007.

1.2 Planteamiento del problema

1.2.1 Identificación del problema

Las legislaciones relacionadas a la protección de datos personales ha ido avanzando a grandes pasos a nivel global; sin embargo, el cumplimiento intrínseco del respeto a la privacidad ha sido lento por la necesidad de estándares que permitan proteger el derecho a la privacidad de las personas en este mundo interconectado (Maqueo Ramírez, Moreno González, & Recio Gayo, 2017).

Según Cruzatt "el derecho a la protección de datos de carácter personal se caracteriza por ser un derecho de contenido complejo (…)". (Cruzatt, 2005).

De acuerdo Global de Riesgos 2017 del Foro Económico Mundial, uno de los mayores impacto y probabilidad de ocurrencia son los ciberataques y el robo de información realizadas por personas externas e internas. (World Economic Forum, 2017).

En el Perú, la obligatoriedad de la Ley de Protección de Datos Personales (LPDP) nro. 29733 es para empresas públicas y privadas, dentro de su alcance se encuentran las universidades que traten datos personales de alumnos, docentes, personal administrativo, proveedores y otros. La LPDP fue publicada el 3 de julio de 2011 en el Diario Oficial, El Peruano, esta Ley tiene como objeto: "Garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del

Perú, a través de su adecuado tratamiento" (Congreso de la República del Perú, 2011, p. 1).

Posteriormente, el Reglamento de la LPDP fue aprobado el 22 de marzo de 2013 por DECRETO SUPREMO Nº 003-2013-JUS (Autoridad Nacional de Protección de Datos Personales, 2013, p. 1), complementado y extendiendo la Ley para su aplicación.

La UPeU es persona jurídica de derecho privado, según el Artículo 1º de su Estatuto (Estatuto UPeU, 2017, p. 1). Por lo tanto, como Titular de sus Bancos de Datos tiene por obligación cumplir con los siguientes principios rectores de la tabla 1.

Tabla 1
Principios rectores de la Ley de Protección de Datos Personales

Principio Rector	**Acción**
Artículo 4. Principio de legalidad	Recopilar datos por medios legales y lícitos
Artículo 5. Principio de consentimiento	Obtener consentimiento del titular del dato
Artículo 6. Principio de finalidad	Establecer alcances de la finalidad de los datos
Artículo 7. Principio de proporcionalidad	No exceder la finalidad de los datos recopilados
Artículo 8. Principio de calidad	Obtener datos veraces, exactos y actualizados
Artículo 9. Principio de seguridad	**Adoptar medidas técnicas, organizativas y legales**
Artículo 10. Principio de disposición de recurso	Contar con vías jurisdiccionales para reclamos y ejercer los derechos del titular del dato personal
Artículo 11. Principio de nivel de protección adecuado	Garantizar la protección de datos para el flujo transfronterizo de datos.

La UPeU ha ido avanzando en el cumplimiento de la LPDP, pero aún no ha desarrollado estrategias para el cumplimiento del Artículo 9. Principio de seguridad. Ante lo mencionado se identificó dos Bancos de Datos Personales; Primero, el Banco de Datos

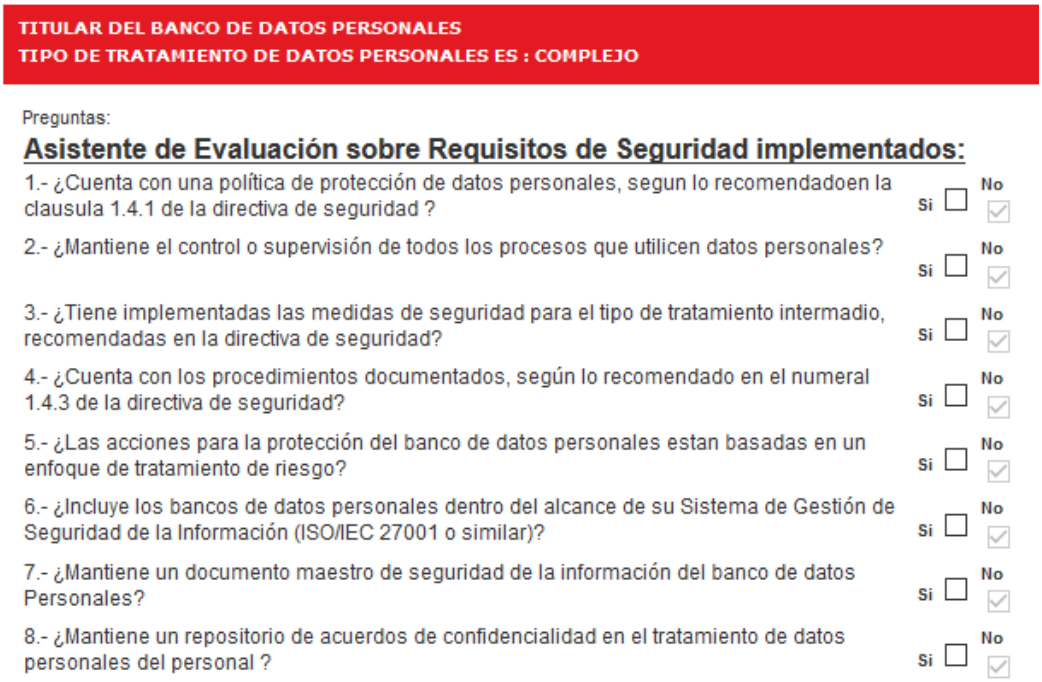
Personales Automatizado ubicado en el área de DIGETI; Segundo, el Banco de Datos Personales No Automatizado ubicado en el área de SG.

En una visita preliminar a DIGETI en su área de Redes y Conectividad, se pudo obtener mediante una evaluación de "Seguridad Física y Ambiental de la Información", que la protección de respaldos de la información se realiza de manera inadecuada, según el Artículo 40 del Reglamento de la LPDP: "Los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados" (Autoridad Nacional de Protección de Datos Personales, 2013); esto se suma al incidente ocurrido en el año 2012, donde se perdió la información personal de los usuarios del área de biblioteca, según el personal afectado no se tuvo una buena gestión para la protección de los respaldos de la información (Sánchez, 2016).

Otra punto crítico encontrado, es el deficiente control de acceso a los sistemas que contienen información personal, como por ejemplo: el Portal Académico (Intranet); si bien el Área de Desarrollo se encarga de otorgar los accesos y privilegios, no se puede asegurar un control sobre los usuarios y el uso que realizan con los mismos, además que no se cuenta con políticas de control de acceso establecidas, ya sea por desconocimiento o por responsabilidad propia, algo que se especifica explícitamente en la disposición nro. 11 de la NTP-ISO/IEC 17799:2007: "Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio" (ISO/IEC, 2007, sec. 11), haciendo referencia al Artículo 39 del Reglamento de la LPDP (Autoridad Nacional de Protección de Datos Personales, 2013, Art. 39).

En Secretaría General se evidenció que realizan transferencia de datos personales sin autorización del Titular o Encargado del Banco de Datos. Así mismo, ocurrió casos que personas no autorizadas ingresaron al "Archivo Institucional", lugar donde se almacenan datos personales sensibles y de única versión (Huamán, 2016).

En la siguiente figura 1 se aprecia los requisitos de seguridad que el titular del banco de datos personales debería implementar y su incumplimiento ante cada uno de ellos (MINJUS, Asistente de Evaluación, 2016).



TITULAR DEL BANCO DE DATOS PERSONALES
TIPO DE TRATAMIENTO DE DATOS PERSONALES ES : COMPLEJO

Preguntas:

Asistente de Evaluación sobre Requisitos de Seguridad implementados:

1.- ¿Cuenta con una política de protección de datos personales, segun lo recomendadoen la clausula 1.4.1 de la directiva de seguridad ?	Si ☐	No ☑
2.- ¿Mantiene el control o supervisión de todos los procesos que utilicen datos personales?	Si ☐	No ☑
3.- ¿Tiene implementadas las medidas de seguridad para el tipo de tratamiento intermadio, recomendadas en la directiva de seguridad?	Si ☐	No ☑
4.- ¿Cuenta con los procedimientos documentados, según lo recomendado en el numeral 1.4.3 de la directiva de seguridad?	Si ☐	No ☑
5.- ¿Las acciones para la protección del banco de datos personales estan basadas en un enfoque de tratamiento de riesgo?	Si ☐	No ☑
6.- ¿Incluye los bancos de datos personales dentro del alcance de su Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001 o similar)?	Si ☐	No ☑
7.- ¿Mantiene un documento maestro de seguridad de la información del banco de datos Personales?	Si ☐	No ☑
8.- ¿Mantiene un repositorio de acuerdos de confidencialidad en el tratamiento de datos personales del personal ?	Si ☐	No ☑

Figura 1. Asistente de Evaluación sobre Requisitos de Seguridad implementados (**Fuente*:*** https://bancodatos.minjus.gob.pe/bancodatos_web/TratamientoWebAction_verTratamientoWeb)

Por lo mencionado, se contempla que existe un "Bajo nivel de cumplimiento de medidas de seguridad para la protección de datos personales en la Universidad Peruana Unión", exigidos por el Artículo 16 de la Ley: "Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado" (Congreso de la República del Perú, 2011, Art. 16).

1.2.2 Problema General

¿La implementación de los controles de seguridad basado en la NTP-ISO/IEC 17799:2007 permite el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Implementar controles de seguridad basado en la NTP-ISO/IEC 17799:2007 para el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada.

1.3.2 Objetivos específicos

- Realizar una evaluación preliminar de cumplimiento del Reglamento de la LPDP en DIGETI y SG.
- Desarrollar un plan de mejora basado en los controles de seguridad de acuerdo a la NTP-ISO/IEC 17799:2007.
- Implementar controles de seguridad para el cumplimiento del Capítulo V "Medidas de Seguridad" del Reglamento de la LPDP.
- Realizar una evaluación al área comprometida para identificar el nivel de cumplimiento post implementación.
- Evidenciar mediante entregables el nivel de mejora alcanzado en las medidas de seguridad para la protección de datos personales.

1.4 Hipótesis

1.4.1 Hipótesis general

La implementación de controles de seguridad basado en la NTP-ISO/IEC 17799:2007 permite el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada.

1.4.2 Hipótesis específicas

- La realización de una evaluación preliminar determina los puntos de no cumplimiento del Reglamento de la LPDP en DIGETI y SG.

- El desarrollo del plan de mejora se basa en los controles de seguridad de la NTP-ISO/IEC 17799:2007.
- La implementación de los controles de seguridad permite el cumplimiento del Capítulo V “Medidas de Seguridad” del Reglamento de la LPDP.
- La realización de una evaluación post implementación determina el nivel de mejora.
- Los entregables evidencian el nivel de mejora alcanzado en las medidas de seguridad para la protección de datos personales.

1.5 Operacionalización de variables

1.5.1 Identificación de variables

1.5.1. Variable dependiente

La variable dependiente son los artículos del Capítulo V “Medidas de Seguridad” del Reglamento de la LPDP.

1.5.2. Variable independiente

La variable independiente son los controles de seguridad de la NTP-ISO/IEC 17799:2007.

1.6 Matriz de consistencia

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS GENERAL	VARIABLE DEPENDIENTE	DIMENSIONES	INDICADORES
¿La implementación de los controles de seguridad basado en la NTP-ISO/IEC 17799:2007 permite el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada?	Implementar controles de seguridad basado en la NTP-ISO/IEC 17799:2007 para el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada.	La implementación de controles de seguridad basado en la NTP-ISO/IEC 17799:2007 permite el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada.	Capítulo V "Medidas de Seguridad" del Reglamento de la LPDP.	1. Medidas de seguridad para el Banco de Datos Personales automatizado. 2. Medidas de seguridad para el Banco de Datos Personales no automatizado.	1. Nivel de cumplimiento exigido por la Ley para el ámbito automatizado 2. Nivel de cumplimiento exigido por la Ley para la ámbito no automatizado
	OBJETIVO ESPECIFICO	**HIPOTESIS ESPECIFICO**	**'ARIABLE INDEPENDIENT**	**DIMENSIONES**	**INDICADORES**
	Realizar una evaluación preliminar de cumplimiento del Reglamento de la LPDP en DIGETI y S.G.	La realización de una evaluación preliminar determina los puntos de no cumplimiento del Reglamento de la LPDP en DIGETI y S.G.	Controles de seguridad de la NTP-ISO/IEC 17799:2007	Aspectos organizativos para la seguridad	Roles y/o Responsabilidades
	Desarrollar un plan de mejora basado en los controles de seguridad de acuerdo a la NTP-ISO/IEC 17799:2007.	El desarrollo del plan de mejora se basa en los controles de seguridad de la NTP-ISO/IEC 17799:2007.		Gestión de comunicación y operaciones	Autorizaciones de transferencia de datos personales
	Implementar controles de seguridad para el cumplimiento del Capítulo V "Medidas de Seguridad" del Reglamento de la LPDP.	La implementación de los controles de seguridad permite el cumplimiento del Capítulo V "Medidas de Seguridad" del Reglamento de la LPDP.		Gestión de incidentes en la seguridad de la información	Procedimientos
				Control de accesos	Formatos para otorgar y retirar accesos
	Realizar una evaluación al área comprometida para identificar el nivel de cumplimiento post implementación.	La realización de una evaluación post implementación determina el nivel de mejora.		Seguridad física y del entorno	Compromisos de confidencialidad
	Evidenciar mediante entregables el nivel de mejora alcanzado en las medidas de seguridad para la protección de datos personales.	Los entregables evidencia el nivel de mejora alcanzado en las medidas de seguridad para la protección de datos personales.		Política de seguridad	Políticas
				Cumplimiento	Leyes afectadas

Figura 2. Matriz de consistencia (**Fuente:** Elaboración propia)

1.7 Justificación

1.7.1 Justificación metodológica

La metodología aplicada abarca la visión end to end de la investigación (Herrero, 2012). El uso de la NTP-ISO/IEC 17799:2007 como un documento de buenas prácticas para la seguridad de la información (ISO/IEC, 2007) contribuye significativamente para la implementación de controles de acuerdo a la necesidad de la UPeU. Así mismo, se utilizó el Ciclo Plan, Do, Check, Act (PDCA: Planificar, Hacer, Verificar y Actuar) para generar la mejora continua en el proyecto y posteriormente en la organización (Jimeno Bernal, 2013).

1.7.2 Justificación tecnológica

La presente investigación tiene como fin diseñar, desarrollar e implementar controles como: procedimientos, formatos y políticas de seguridad que garanticen el tratamiento físico y lógico de los datos personales basados en la NTP- ISO/IEC 17799:2007; garantizando la continuidad del negocio y minimizando los riesgos (Gaspar Martínez, 2016).

1.7.3 Justificación social

El impacto social tendrá un efecto positivo adaptando una cultura de protección de datos en los colaboradores que integran las áreas de aplicación. De la misma manera, la implementación de controles de seguridad para el cumplimiento del Capítulo V "Medidas de Seguridad", generará una iniciativa para el desarrollo de una estrategia que abarque el cumplimiento total de la LPDP en la universidad, evitando sanciones por la Autoridad Nacional de Protección de Datos Personales (ANPDP) y mejorando los servicios de la organización (Plaza, 2015).

1.8 Alcances de la investigación

El alcance de la investigación comprende los siguientes puntos:

- El cumplimiento del Capítulo V "Medidas de Seguridad" del Reglamento de LPDP.
- El desarrollo de controles en base a las cláusulas de la NTP-ISO/IEC 17799:2007.
- La implementación de controles para el Banco de Datos Automatizado en el área de DIGETI.
- La implementación de controles para el Banco de Datos No Automatizado en el área de SG.

CAPÍTULO II: MARCO TEÓRICO CONCEPTUAL

2.1. Marco teórico

2.1.1. Historia de protección de datos

El término “privacidad” inicia con auge en 1890 en los Estados Unidos de América, en el paper “The right of privacy” escrito por Samuel Warren y Louis Brandeis, en este artículo ellos reconocen el derecho a la protección de la información personal, y dejaron abierto el debate en materia de privacidad en países como Francia, Estados Unidos y al rededores (López Torres, 2010).

La Asamblea General de las Naciones Unidas en 1948 adopta el documento conocido en todo el mundo como Declaración Universal de Derechos Humanos, en este documento el Artículo 12 señala que: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques” (ONU, 1948, Art. 12).

Posteriormente, el Convenio del Consejo de Europa, también conocido como “Council of Europe”, realizó el Tratado nro. 108 con el título: “Convenio para la Protección de las Personas con Respecto al Tratamiento Automático de Datos Personales”; este convenio es el primer tratado internacional que protege a la persona ante la recopilación ilegal de las corporaciones, así mismo busca que el procesamiento de los datos personales mantengan un nivel de seguridad alto y regula el flujo transfronterizo, prohibiendo la transferencia de datos personales sensibles y confidenciales (Council of Europe, 1981).

2.1.2. Legislación de protección de datos en el mundo

Según estudios de la Universidad Nacional Autónoma de México, existen dos enfoques principales de protección de datos personales; el primer modelo es el europeo que busca proteger la información y su propiedad, priorizando los derechos humanos de las personas; el segundo modelo es el estadounidense que se centra en la información de las personas con el derecho a su privacidad, regulando el tratamiento y finalidad de las empresas que lucran sin distinción con esa información (Sánchez Pérez & Rojas González, 2017).

En la siguiente figura 3 se aprecia como alrededor del mundo se han promulgado leyes de protección de datos. Es importante mencionar que cada país es un caso distinto, donde formulan sus legislaciones en base a sus condiciones culturales, económicas y políticas.

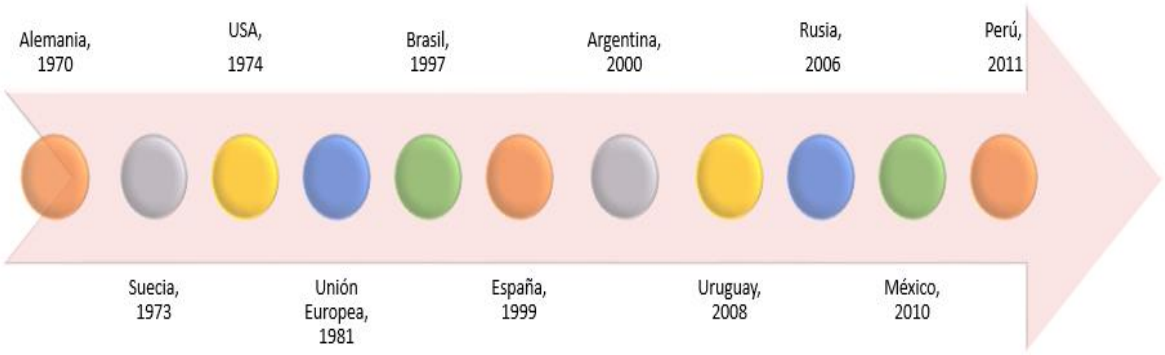


Figura 3. Línea de tiempo de países que promulgaron leyes en materia de protección de datos (**Fuente:** Elaboración propia)

En América Latina existen distintos casos de iniciativas de privacidad; algunos países tienen la Ley, pero no está reglamentada; otro caso es la creación de una Autoridad de Protección de Datos, pero no existe legislación al respecto. La siguiente figura 4 muestra las diferencias y avances en legislación de protección de datos en países de América Latina.

N°	PAIS	No tiene Ley	Habeas Data	Ley Aprobada	Autoridad nacional de protección y/o supervisión	Registro nacional de bancos de datos personales	Nivel de madurez	Comentario
1	ARGENTINA		X	X	X	X	OPTIMIZADO	
2	BOLIVIA		X				INICIADO	
3	BRASIL		X				INICIADO	
4	CANADÁ			X	X		GESTIONADO-	SIN HABEAS DATA
5	CHILE		X	X		X	OPTIMIZADO-	SIN AUTORIDAD NACIONAL
6	COLOMBIA		X	X	X	X	OPTIMIZADO	
7	COSTA RICA		X	X	X	X	OPTIMIZADO	
8	ECUADOR		X	X		X	OPTIMIZADO-	SIN AUTORIDAD NACIONAL
9	EL SALVADOR	X					INEXISTENTE	
10	ESTADOS UNIDOS		X	X	X		GESTIONADO	
11	GUATEMALA		X				INICIADO	
12	MEXICO		X	X	X	X	OPTIMIZADO	
13	PANAMA	X					INEXISTENTE	
14	PERU		X	X	X	X	OPTIMIZADO	
15	PARAGUAY		X	X			DEFINIDO	
16	REPUBLICA DOMINICANA		X	X			DEFINIDO	

Figura 4. Legislación de Protección de Datos Personales en América Latina (**Fuente:** https://www.linkedin.com/pulse/d%25C3%25ADa-internacional-de-la-protecci%25C3%25B3n-datos-personales-g%25C3%25B3mez-morales/)

2.1.3. Legislación de protección de datos en el Perú

2.1.3.1. Marco general

Para iniciar a hablar de la LPDP en el territorio peruano, debemos de contemplar el contexto en el cual fue creada.

La Constitución Política del Perú, en su Artículo 2 numeral 6 señala que: “Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecten a la intimidad personal y familiar.” (Congreso Constituyente del, 1993, Art. 2). Es por esto que el Congreso de la República del Perú aprobó el 7 de junio de 2010 el Proyecto de Ley N° 4079/2009-PE que propone la LPDP. De esta manera es que, el 3 de Julio del 2011 es publicado en el Diario Oficial “El Peruano” la Ley N° 29733 Ley de Protección de Datos Personales (Congreso de la República del Perú, 2011). La siguiente figura 5 muestra el organigrama de la Dirección General de Protección de Datos Personales (DGPDP).

Figura 5. Organigrama de la DGPDP (**Fuente**: Elaboración propia)

Esta Ley consta de un título preliminar con disposiciones generales, 40 artículos y 11 disposiciones complementarias legales; el objetivo de la LPDP es el de: Garantizar el derecho fundamental a los datos personales realizando un adecuado tratamiento a los mismos; esto implica el respeto de los derechos fundamentales, así como las normas contempladas en la LPDP y su Reglamento.

Los datos personales sujetos a la LPDP son los que hacen identificable a toda persona natural, eso quiere decir que todo registro o información obtenida de personas jurídicas no se encuentra sujeta a esta Ley (Juape, 2015). En la siguiente figura 6 se aprecian ejemplos de datos personales, relacionados a la salud y sensibles según el Reglamento de la LPDP.

Datos personales	Nombres y Apellidos
	Fecha de nacimiento
	Fotografía o video de una persona
	Hábitos personales
Datos relacionados a la salud	Información genética
	Estado físico o mental
	Discapacidad
	Salud pasada, presente o pronosticada
Datos sensibles	Salario
	Creencia religiosa o filosófica
	Moral o emocional
	Afectiva o familiar

Figura 6. Datos Personales según el Reglamento de la LPDP (**Fuente:** Elaboración Propia)

Así mismo el 22 de marzo del 2013, mediante un Decreto Supremo se aprobó el Reglamento de la Ley N° 29733, el cual muestra en detalle las disposiciones de la Ley; ésta entra en vigencia desde el 8 de mayo, tras 30 días hábiles después de su evaluación. (Autoridad Nacional de Protección de Datos Personales, 2013)

La LPDP abarca entidades públicas, compañías del sector privado, personas naturales y su alcance está sobre los datos personales destinados a incluirse en Bancos de Datos, estos están a cargo de un Titular del Banco de Datos en el territorio peruano.

2.1.3.2. Medidas de seguridad

El Artículo 16 de la LPDP menciona: "Para fines de tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado" (Congreso de la República del Perú, 2011, Art 16).

Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la ANPDP, salvo la existencia de disposiciones especiales contenidas en otras leyes" (Congreso de la República del Perú, 2011) . Por lo que para cumplir con este aspecto de la Ley se deben revisar los requisitos encontrados en su Reglamento.

Las medidas de seguridad a las que se refiere la LPDP están descritas en el "Título V" de su Reglamento y abarcan desde el Artículo 39 al 46 del mismo.

A. Medidas de seguridad en ámbitos automatizados

Se puede encontrar los siguientes:

- **Control de acceso**

Contar con una adecuada identificación de los Usuarios que tienen acceso a los sistemas que contienen Información personal; esto mediante: usuario-contraseña, uso de certificados digitales, tokens, entre otros).

Realizar una correcta gestión de los privilegios, revisiones periódicas de los permisos y que cuenten con procedimientos documentados, que definen los aspectos anteriores.

- **Trazabilidad**

  Debe realizarse un mantenimiento de registros: usuario, hora de inicio y cierre de sesión y acciones relevantes; mantener una gestión de las trazas: disponibilidad oportuna, almacenamiento, destrucción, transferencia (Deloitte, 2015)

- **Gestión de respaldos y conservación**

  En cuanto a los medios en los cuales se almacena información de respaldo la normativa contempla lo siguiente: Ambientes en los que se procese o almacene o transmita la información, se deben de considerar las recomendaciones de seguridad física y ambiental recomendadas en la NTP-ISO/IEC 17799:2007. Así mismo, menciona que los respaldos y pruebas de recuperación deben ser verificables.

- **Transferencias**

  Todo envío de Información al exterior de las instalaciones físicas de la institución y que contenga Datos Personales debe contar con la Autorización del titular del BDP. Así mismo para la protección de los envíos se debe contar con mecanismos de protección como, por ejemplo: cifrado, checksum u otras tecnologías.

B. Medidas de seguridad en ámbitos no automatizados

Las medidas técnicas no automatizadas se refieren a cualquier información que no se encuentren en soportes lógicos o digitales.

- **En almacenamiento**

  Los armarios y archivadores deben encontrarse en áreas de acceso restringido, y estas deben siempre mantenerse cerradas con mecanismos de seguridad apropiadas para salvaguardar la información.

- **Copias de documentos**

  Las copias de los documentos que contengan información personal sólo podrán realizarse bajo el control del personal autorizado.

  Las copias en desuso que contienen datos personales deben ser destruidas.

- **Acceso a documentos**

  El acceso a los documentos debe ser solo por personal autorizado, se debe contar con un registro de accesos en el caso de que varios usuarios vayan a acceder a los documentos.

- **Traslado de documentos**

  Para el traslado de documentos se deben contar con medidas para impedir el acceso o manipulación indebida en el proceso.

2.1.3.3. Sanciones

En el Artículo 37 y 38 de la LDPD describe que el encargado de supervisar las infracciones y sanciones cometidas por cualquier entidad es la ANPDP; esta inicia el procedimiento sancionador por parte suya o por denuncia de un tercero ante la presunta evidencia de actos contra lo dispuesto en la Ley o su Reglamento (Autoridad Nacional de Protección de Datos Personales, 2013; Congreso de la República del Perú, 2011)

Las sanciones son clasificadas en tres niveles: infracciones leves, graves, y muy graves; en este caso por el incumplimiento de no contar con las correctas medidas de seguridad serían las siguientes.

A. Infracciones Graves:

Las infracciones graves son sancionadas con multa desde más de cinco Unidades Impositivas Tributarias (UIT) hasta cincuenta UIT.

Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento (Congreso de la República del Perú, 2011, Art. 38)

B. Infracciones Muy Graves:

Las infracciones muy graves son sancionadas con multa desde más de 50 UIT hasta 100 UIT.

La sección 1 menciona que: "Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales" (Congreso de la República del Perú, 2011, Art. 38, sec 1).

La sección 2 menciona que: "Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido por la presente Ley o su reglamento" (Congreso de la República del Perú, 2011, Art38, sec. 2).

La Ley también describe que "la multa impuesta en ningún caso debe exceder el 10% de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior". Así mismo la ANPDP puede imponer multas coercitivas que no superen las 10 UIT por el no cumplimiento de las sanciones ya impuestas. Las multas se imponen una vez vencido el plazo del cumplimiento (Congreso de la República del Perú, 2011, Art. 39).

2.1.4. Seguridad de la Información

2.1.4.1.NTP-ISO/IEC 17799:2007

La Norma Técnica Peruana NTP-ISO/IEC 17799 es un documento que contiene buenas prácticas de gestión de la seguridad de la información. Su propósito es presentar

una serie de recomendaciones para realizar una correcta gestión de seguridad de la información y servir de guía para adoptar o implementar estándares de seguridad en las organizaciones (ISO/IEC, 2007).

Su uso fue dispuesto por la Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) el 23 de Julio del 2004. La siguiente tabla 2 detalla la NTP-ISO/IEC 17799 que cuenta con 11 cláusulas de control de seguridad con 39 categorías contenidas en estas; dicha norma fue actualizada el 25 de agosto del 2007 como la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI.

Tabla 2
Dominios, objetivos de control y categorías principales NTP-ISO/IEC 17799:2007

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	CANTIDAD DE CONTROLES
1	POLÍTICA DE SEGURIDAD	1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	2
2	ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	2.1 ORGANIZACIÓN INTERNA	8
		2.2 SEGURIDAD EN LOS ACCESOS DE TERCERAS PARTES	3
3	CLASIFICACIÓN Y CONTROL DE ACTIVOS	3.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	3
		3.2 CLASIFICACIÓN DE LA INFORMACIÓN	2
4	SEGURIDAD EN RECURSOS HUMANOS	4.1 SEGURIDAD ANTES DEL EMPLEO	3
		4.2 DURANTE EL EMPLEO	3
		4.3 FINALIZACIÓN O CAMBIO DEL EMPLEO	3

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	CANTIDAD DE CONTROLES
5	SEGURIDAD FÍSICA Y DEL ENTORNO	5.1 ÁREAS SEGURAS	6
		5.2 SEGURIDAD DE LOS EQUIPOS	5
6	GESTIÓN DE COMUNICACIONES Y OPERACIONES	6.1 PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIONES	4
		6.2 GESTIÓN DE SERVICIOS EXTERNOS	3
		6.3 PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA	2
			3
		6.4 PROTECCIÓN CONTRA SOFTWARE MALICIOSO	1
			2
		6.5 GESTIÓN DE RESPALDO Y RECUPERACIÓN	4
		6.6 GESTIÓN DE SEGURIDAD EN REDES	5

		6.7 Utilización de los medios de información	3
		6.8 Intercambio de información	6
		6.9 Servicios de correo electrónico	
		6.10 Monitoreo	

ÍTEMS	DOMINIOS	OBJETIVOS DE CONTROL	CANTIDAD DE CONTROLES
7	Control de accesos	7.1 Requisitos de negocio para el control de acceso	1
		7.2 Gestión de acceso de usuarios	4
		7.3 Responsabilidades de los usuarios	3
		7.4 Control de acceso a la red	7
		7.5 Control de acceso al sistema operativo	6
		7.6 Control de acceso a las aplicaciones y la información	2
		7.8 Informática móvil y teletrabajo	2
8	Adquisición, desarrollo y mantenimiento de sistemas	8.1 Requisitos de seguridad de los sistemas	1
		8.2 Seguridad de las aplicaciones del sistema	4
		8.3 Controles criptográficos	2
		8.4. Seguridad de los archivos del sistema	3
		8.5 Seguridad en los procesos de desarrollo y soporte	5
		8.6 Gestión de la vulnerabilidad técnica	1
9	Gestión de incidentes en la seguridad de información	9.1 Reportando eventos y debilidades de la seguridad de la información	2
		9.2 Gestión de las mejoras e incidentes en la seguridad de la información	3
10	gestión de continuidad del negocio	10.1 Aspectos de la gestión de continuidad del negocio	5
11	Cumplimiento	11.1 Cumplimiento con los requisitos legales	6
		11.2 Revisiones de la política de seguridad y de la conformidad técnica	2
		11.3 Consideraciones sobre la auditoría de sistemas	1

Esta norma técnica se caracteriza por su flexibilidad, pues no induce a las organizaciones a cumplir lo estipulado al pie de la letra, si no que les permite encontrar soluciones de seguridad de acuerdo a las necesidades (Conexión ESAN, 2016)

Según el especialista de la ONGEI, Max Lázaro, las recomendaciones de la norma son neutrales en cuanto a la tecnología. Por ejemplo: La norma propone la necesidad de contar con Firewalls, pero no especifica sobre los tipos de Firewalls a aplicar y cómo se utilizan. Por lo que la NTP-ISO/IEC 17799:2007 fue emitida para ser considerada en la implementación de estrategias y planes de seguridad de la información.

Los controles de seguridad de la NTP-ISO/IEC 17799:2007 a destacar para el desarrollo de nuestra investigación se encuentran en los siguientes dominios:

A. Aspectos organizativos para la seguridad

El objeto de este dominio es el de gestionar la seguridad de la información en la organización. Para la presente investigación usamos el control para la asignación de responsabilidades sobre la seguridad de la información; acuerdos de confidencialidad para mantener el compromiso de los colaboradores con la no divulgación de la información: y los controles derivados de la seguridad en los accesos de terceras partes.

B. Seguridad física y del entorno

En este apartado quedan recogidas las medidas de seguridad física y del entorno, y las divide en dos controles:

- Por una parte, se muestran los requerimientos de seguridad físicos en los edificios, como el establecer un perímetro de seguridad, los controles de ingreso físicos, protección contra amenazas físicas externas, o los controles de seguridad en las zonas de entrega y carga.
- Por la otra, la seguridad de los equipos, servicios públicos de soporte, seguridad en el cableado, el mantenimiento de los equipos, la seguridad de equipos fuera del

local, así como la seguridad de la eliminación o re-uso del equipo y el retiro de la propiedad.

C. Gestión de Comunicación y Operaciones

Para la comunicación de las operaciones debe contar con procedimientos debidamente establecidos, estos procedimientos deben mostrar de manera clara las responsabilidades.

En este apartado también e incluyen las recomendaciones en cuanto a los respaldos o Backups, la gestión en la seguridad de la red y algo muy importante que es el intercambio de la información y el monitoreo (auditorías) sobre las actividades establecidas en cuanto a seguridad.

D. Gestión de incidentes en la seguridad de la información

Para el proyecto de investigación se usó los controles de este dominio para reportar formalmente eventos y debilidades de seguridad de la información ocurridos en el área comprometida, así mismo, para que se pueda realizar acciones correctivas y hacerse de conocimiento al titular del dato personal o a la administración de la organización según sea el caso.

E. Política de seguridad

El dominio de Política de Seguridad tiene como objetivo administrar y ayudar en la gestión de la seguridad de la información. Otro aspecto resaltante que menciona la NTP es el estar en concordancia con las necesidades de la organización y cumplir con las legislaciones. La presente investigación hace uso de este dominio, estableciendo formas claras de actuación y de entendimiento para los empleados afectados por el área respectiva.

F. Control de accesos

En esta cláusula se presentan pautas para tener en cuenta respecto al acceso a las redes, a los sistemas que contienen información, a los sistemas operativos y a las diversas

aplicaciones corporativas. De la misma manera la correcta gestión de los privilegios de los usuarios y las responsabilidades que cada uno para el manejo correcto de la información.

G. Cumplimiento

El objetivo de este dominio es el de cumplir con las legislaciones vigentes dependiendo del modelo de negocio de la organización y sus necesidades. La LPDP está dentro del alcance de este dominio, por la tanto se consideró los controles de este apartado para lograr el cumplimiento de la LPDP y el respeto por la privacidad.

2.1.4.2. Directiva de Seguridad

La Directiva de Seguridad es un documento elaborado por la ANPDP (Autoridad Nacional de Protección de Datos Personales) para facilitar el cumplimiento de normas de seguridad o algún criterio, así mismo la ANPDP enfatiza que este no es un documento para cumplirlo, el foco debe estar centrado en la Ley (Justicia Derechos Humanos, Directiva de Seguridad, 2013).

Esta directiva es altamente recomendable e interesante en cuanto a la implementación de medidas de seguridad técnicas. “La directiva de seguridad no es un simple check-list que sea de aplicación en todos los casos, de hecho, la directiva de seguridad no contempla muchos aspectos específicos de la Ley 29733 (como las características del consentimiento o los principios de la Ley) sino que se centra principalmente en medidas de seguridad, condiciones de seguridad y requisitos” (GTDI, 2015).

Los titulares de los BDP son los principales destinatarios, ya que ellos son los que realizan tratamientos ya sean de tipo básico, simple o intermedio. A su vez estas se focalizan más que todo en hacer recomendaciones para cumplir la Ley que no suponen inversiones importantes.

En cuanto a la relación con la NTP-ISO/IEC 17799, se puede decir que es muy estrecha ya que, para las entidades públicas, se requiere que los Sistemas de Gestión de Seguridad Informática sean implementados en base a la ISO 27001 que no es más que el estándar original usado internacionalmente.

En conclusión, el documento de Directivas de Seguridad es de mucha ayuda a las organizaciones para el cumplimiento de la LPDP, pero en situaciones de empresas con necesidades mayores se usarán otros mecanismos para el cumplimiento de la LPDP.

2.2. Marco conceptual

2.2.1. Conceptos generales de la Ley nro. 29733

La LPDP para efectos de su entendimiento menciona las siguientes definiciones:

2.2.1.1. Banco de datos personales

Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

2.2.1.2. Banco de datos personales de administración privada

Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.

2.2.1.3. Datos personales

Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

2.2.1.4. Datos sensibles

Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos,

opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual

2.2.1.5. Encargado del banco de datos personales

Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales

2.2.1.6. Titular del banco de datos personales

Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

2.2.1.7. Flujo transfronterizo de datos personales

Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

2.2.1.8. Titular de datos personales

Persona natural a quien corresponde los datos personales.

2.2.1.9. Transferencia de datos personales

Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

2.2.1.10. Tratamiento de datos personales

Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por

transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

2.2.1.11. Autoridad de Protección de Datos Personales

Es el órgano correspondiente de realizar todas las acciones necesarias para que se asegure el cumplimiento de la legislación vinculada directamente con la Protección de Datos Personales y sus principios rectores.

2.2.2. Conceptos de Seguridad

2.2.2.1. Seguridad Física

La Seguridad Física se entiende por cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado un sistema o en este caso un banco de datos. Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.
- Disturbios internos y externos.

Evaluar y controlar de manera permanente la seguridad física del sistema es el primer paso para comenzar a integrar la seguridad como función primordial en la organización. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes.

2.2.2.2. Seguridad Lógica

La Seguridad Lógica es la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en los sistemas (Seguridad Física y Lógica, 2016). Los objetivos a cumplir de la Seguridad Lógica son:

- Restringir el acceso a los programas y archivos.

- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

CAPÍTULO III: METODOLOGÍA Y MATERIALES

3.1. Diseño de la investigación

3.1.1. Metodología de la investigación

La metodología de investigación es la columna vertebral del proyecto, esta comprende 5 etapas de inicio a fin (ver figura 7). En la primera fase se realiza un Análisis GAP a las áreas interesadas; en la segunda fase se planifica la mejora en base a los controles de la NTP-ISO/IEC 17799:2007; en la tercera fase es ejecutar los controles planificados; en la cuarta fase se evalúa los resultados obtenidos de la post implementación; finalmente la quinta fase se determina el nivel de mejora de las “Medidas de Seguridad” del Reglamento de la LPDP.

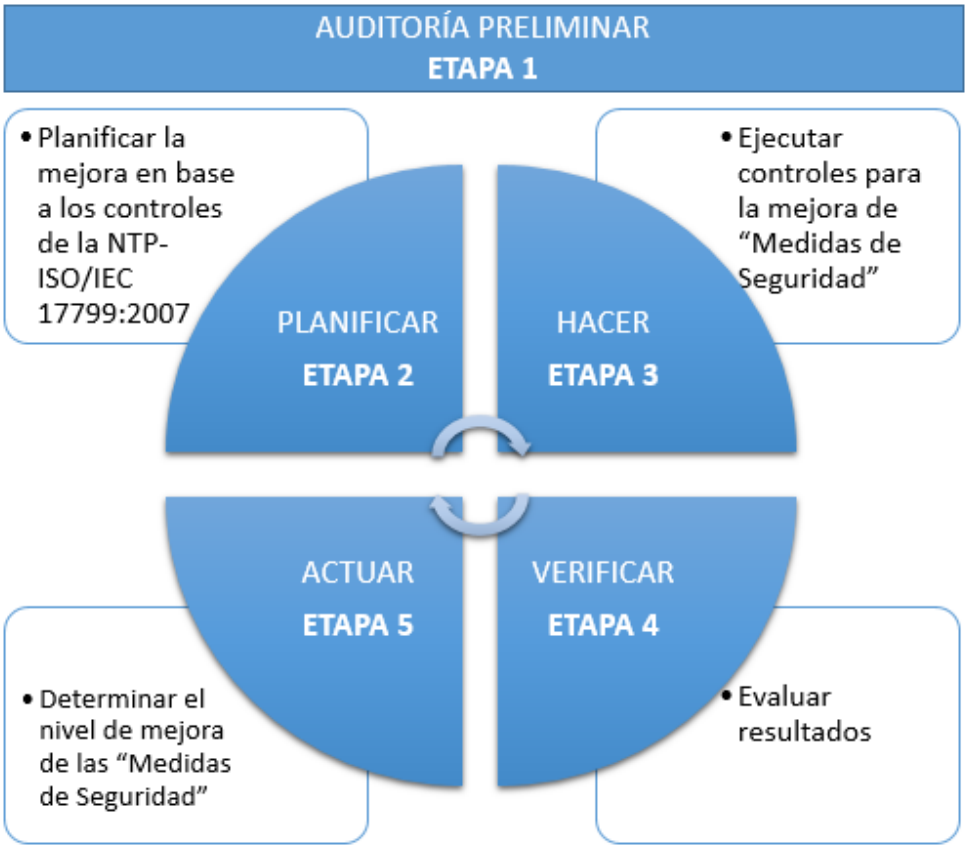


Figura 7. Etapas de la metodología de investigación (**Fuente:** Elaboración propia)

3.1.1.1. Descripción de las etapas de la metodología

A. Etapa 1: Auditoría Preliminar

Esta primera fase se encarga de analizar la situación actual con un Análisis GAP a las áreas interesadas, identificando la brecha de cumplimiento en cuanto a la LPDP. El desarrollo del Análisis GAP consta de una: a) Planificación de auditoría; b) Ejecución de auditoría ;y c) Presentación del dictamen final de auditoría. Ver la siguiente figura 8.

Figura 8. Actividades de la Etapa 1: Auditoría Preliminar (**Fuente**: Elaboración propia)

B. Etapa 2: Planificar

La segunda etapa es Planificar la mejora en base a los controles de la NTP-ISO/IEC 17799:2007, esta constituye en realizar el plan de implementación de los controles que están para el cumplimiento de la LPDP. Las actividades de esta segunda etapa consta en: a) Examinar los artículos del Capítulo V "Medidas de Seguridad" del Reglamento de la Ley para establecer los alcances de cumplimiento b) Analizar los controles de la NTP, evaluando su viabilidad en la organización y el cumplimiento de la Ley; c) Determinar los controles adecuados; d) Elaborar las propuestas de los controles a implementar para las áreas interesadas; y por último e) Elaborar los controles, tales como formatos, políticas, instructivos, procedimientos y otros. Ver la siguiente figura 9.

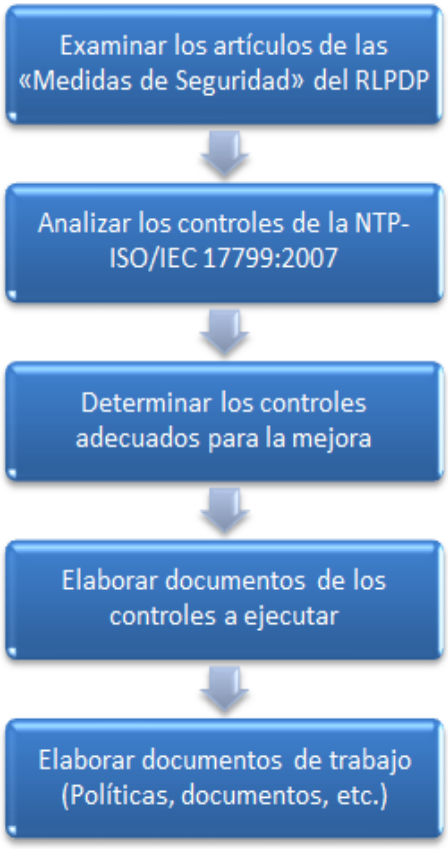


Figura 9. Actividades de la Etapa 2: Planificar (**Fuente**: Elaboración propia)

C. Etapa 3: Hacer

La tercera etapa es Ejecutar controles para la mejora de "Medidas de Seguridad", esta etapa se enfoca en implementación de los controles previamente planificados y elaborados en la Etapa 2, las actividades que comprende esta etapa es: a) Presentar controles de seguridad a la dirección, así mismo, se revisa el documento para su viabilidad en el área y posibles modificaciones; b) Aprobar controles necesarios a implementar con el director o jefe del área involucrada; y e) Concientizar a las personas interesadas con reuniones programadas. Ver la siguiente figura 10.

Figura 10. Actividades de la Etapa 3: Ejecutar (**Fuente**: Elaboración propia)

D. Etapa 4: Verificar

La cuarta etapa es Evaluar resultados, en esta etapa se evalúa los resultados de la post implementación de controles de seguridad. Esta etapa comprende las actividades de la auditoría preliminar detalladas en la figura 8, que en concreto es: a) Planificar la auditoría; y b) Ejecutar la auditoría. Ver la siguiente figura 11.

Figura 11. Actividades de la Etapa 4: Verificar (**Fuente**: Elaboración propia)

E. Etapa 5: Actuar

La quinta etapa es Determinar el nivel de mejora de las “Medidas de Seguridad”. Las actividades comprenden: a) Analizar los resultados post implementación; b) Determinar el nivel de mejora de “Medidas de Seguridad”; adoptar una cultura de seguridad de la información y promover el cumplimiento de la LPDP a nivel corporativo. Ver la siguiente figura 12.

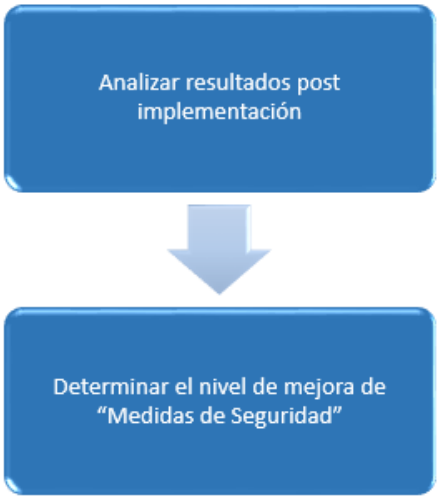


Figura 12. Actividades de la Etapa 5: Actuar (**Fuente**: Elaboración propia)

3.1.2. Nivel de la investigación

El nivel de investigación es descriptivo y experimental. Según Salkind “la investigación descriptiva reseña las características de un fenómeno existente” (Salkind, 1998).

3.1.3. Tipo de la investigación

Hernández, Fernández y Baptista (2003) explican que se clasifica exploratoria cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes.

La investigación es exploratoria por la carencia de investigaciones orientadas al cumplimiento normativo de protección de datos personales. Asimismo, es del tipo explicativo ya que la solución a presentarse será implementada y evaluada; los resultados

obtenidos nos permitirán conocer si es la efectividad de nuestro proyecto en la organización.

3.1.4. Enfoque de la investigación

Es de Enfoque Mixto. Cuantitativo porque los resultados obtenidos en las evaluaciones antes y después de la implementación serán descritos por porcentajes en cuanto al cumplimiento de la LPDP. Así mismo es cualitativo; porque se dio soluciones a partir de del propio análisis, basado en los resultados de las evaluaciones pre y post implementación. Abadellah manifiesta que las investigaciones cualitativas hacen registros narrativos de los fenómenos que son estudiados mediante técnicas como la observación participante y las entrevistas no estructuradas. (Abdellah, 1994).

3.1.5. Dominio de la investigación

El dominio de la investigación es el cumplimiento de la Ley de Protección de Datos Personales.

3.1.6. Población y muestra

3.1.6.1. Población de estudio

La población es el personal de DIGETI y Secretaría General que labora dentro de la UPeU.

3.1.6.2. Determinación de la muestra

Son las personas encargadas de cada sub área perteneciente al lugar de aplicación.

3.1.6.3. Tipo de muestreo

El muestreo utilizado es el “muestreo intencional” donde por criterio seleccionamos como muestra un subconjunto de la población en un momento.

En este tipo de muestreo el investigador tiene previo conocimiento de los elementos poblacionales. Aunque este muestreo es subjetivo, requiere que el investigador conozca los elementos muéstrales, lo que permite que el muestreo sea representativo (Namakforoosh, 2000).

3.1.6.4. Recolección de información

La recolecta de información se realizó en la primera etapa de la investigación: Evaluar el nivel de cumplimiento actual de las "Medidas de Seguridad" y en la etapa tres para evaluar el cumplimiento post implementación de controles.

A. Entrevista

Se realizaron entrevistas como instrumento de recopilación de información, donde se hizo de forma directa, entre el evaluador y el interrogado. Se realizaron entrevistas libres, dirigidas, de exploración, comprobación e informales.

B. Lista de chequeo

Durante las 2 etapas de evaluación (priori y a posteriori) se desarrollaron listas de chequeo. Este tipo de encuesta es de forma específica y con preguntas precisas; permitiendo analizar e interpretar de una mejor forma la información.

CAPÍTULO IV: DIAGNÓSTICO SITUACIONAL

4.1. Identificación del lugar de aplicación

La UPeU es una empresa privada dedicada al rubro de la educación superior, esta cuenta con Autonomía Universitaria que implica: "autonomía de normativa, de gobierno, académica y administrativa" (Estatuto UPeU, 2017, p. 6). Dicha autonomía comprende las dimensiones: Normativa, Gobierno, Académica, Administrativa y Económica. Es decir, la UPeU cuenta con las facultades necesarias para aprobar y poner en funcionamiento reglamentos, normas y políticas a nivel organizacional para el cumplimiento de la LPDP.

4.2. Direccionamiento estratégico

4.2.1. Misión

"Desarrollar personas íntegras, con espíritu de servicio misionero e innovadoras a fin de restaurar la imagen de Dios en el ser humano" (UPeU, sec. Misión).

4.2.2. Visión

"Ser referente por la excelencia en el servicio misionero y la calidad educativa e innovadora en la iglesia y la sociedad..." (UPeU, sec. Visión).

4.2.3. Organización de la universidad privada

La UPeU de acuerdo a su Estatuto Universitario menciona que: "Es una persona jurídica de derecho privado, sin fines de lucro, y con plena autonomía al servicio de la iglesia Adventista del Séptimo Día y del país; organizada, promovida y conducida por su Promotora. La comunidad universitaria está integrada por docentes, estudiantes y graduados. Además, participan en ella, los representantes de su Promotora y el personal administrativo y de servicios conforme a ley (…)" (Estatuto UPeU, 2017, p. 6).

En la figura 13 se aprecia el mapa de procesos de la UPeU, la cual refleja que los procesos de DIGETI y SG son de apoyo a la organización.

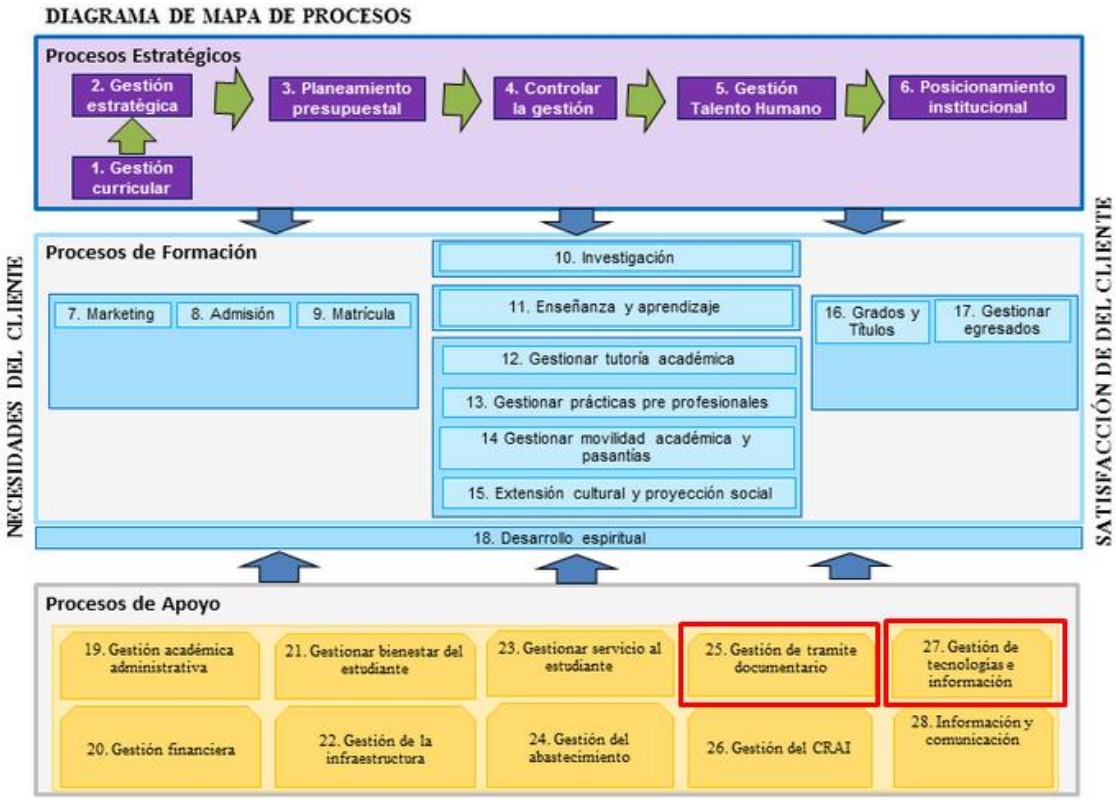


Figura 13. Mapa de Procesos de la UPeU (**Fuente**: http://up.upeu.edu.pe/)

La estructura organizacional de la UPeU manifiesta que el área de DIGETI depende de Vicerrectorado y SG depende de Rectorado. Ver la siguiente figura 14.

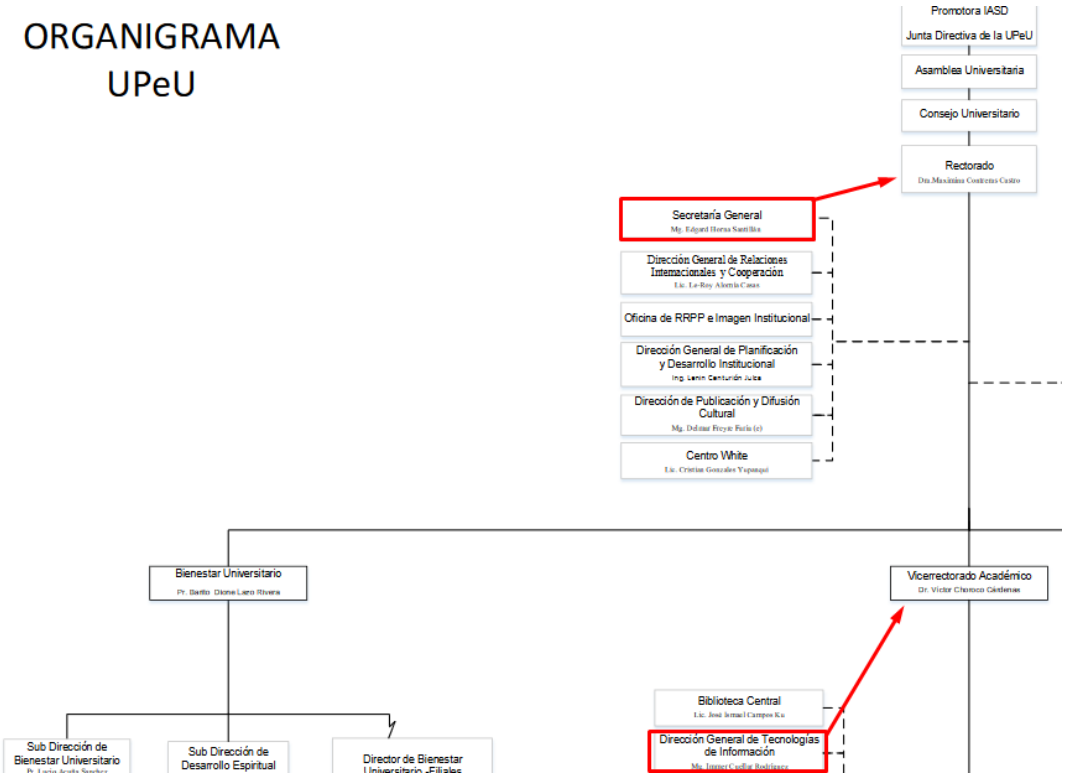


Figura 14. Organigrama institucional de la UPeU (**Fuente:** Organigrama, UPeU, 2017)

4.2.4. Función y estructura de Dirección General de Tecnologías de Información

El área de DIGETI (Dirección General de Tecnologías de Información) es el encargado de velar por la seguridad, controlar y mantener el funcionamiento de las TIC de la UPeU, esta área comprende 4 áreas:

- Área de Redes y Conectividad: Es la encargada de dar apoyo y gestionar las redes de la universidad como también administrar los servidores físicos y virtuales de la UPeU.
- Área de Desarrollo de Software: Es la encargada de dar soporte y mantenimiento a los Sistemas de Información de la UPeU, así mismo, mantiene y otorga accesos especiales al sistema y a los datos personales.
- Área de Mesa de Ayuda: Encargada de brindar servicios de apoyo técnico a alumnos y trabajadores de la universidad, como también la creación y

administración de los usuarios y correos institucionales: Esta área se encarga de brindar servicios de apoyo técnico a alumnos y trabajadores de la universidad, así mismo la creación y administración de los usuarios y correos institucionales.

- Área de Dirección General: Dentro de esta área se encuentran profesionales que coordinan y gestionan: cotizaciones, proyectos, adquisiciones y todo tipo de negociaciones con proveedores.

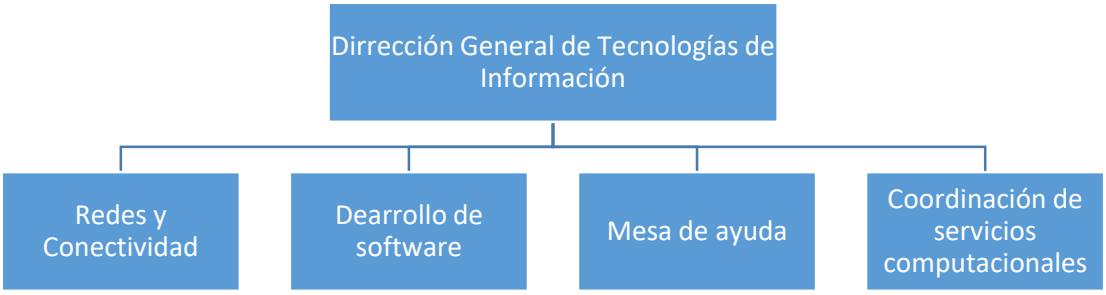


Figura 15. Organigrama de DIGETI (**Fuente**: Elaboración propia)

Por lo tanto, se evidencia que DIGETI realiza tratamiento de datos personales en soporte lógico, que el nivel de criticidad es alto y que es necesario implementar controles de seguridad para la: a) Seguridad en el tratamiento de los datos personales; b) Conservación, respaldo y recuperación de datos personales; c) Transferencia lógica o electrónica de datos personales; d) Prestación de servicios sin acceso a datos personales. Según el Capítulo V "Medidas de Seguridad" del Reglamento de LPDP.

4.2.5. Función y estructura de Secretaria General

Según el Artículo 233º del Estatuto de la UPeU (Estatuto UPeU, 2017, p. 47), el área de Secretaría General es "un órgano de apoyo académico y administrativo a toda la estructura organiza de la Universidad". Así mismo, el Artículo 298º menciona sus unidades administrativas: a) Trámite documentario; b) Grados y títulos, c) Archivo académico general; d) Carné universitario; e) Estadística e información; f) Registros y

actas académicos y g) Registros y actas administrativas.

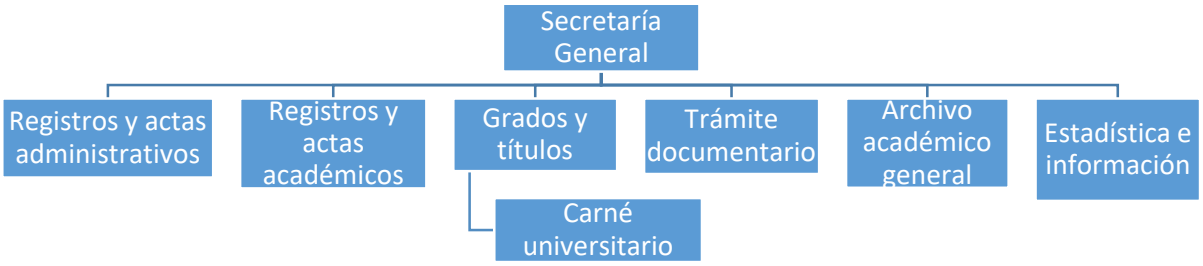


Figura 16. Organigrama de SG (**Fuente:** MOF de Secretaría General)

Las funciones de Secretaría General son:

- Supervisar los trámites y procedimientos académicos administrativos de la Universidad.
- Supervisar las etapas de Proyectar, transcribir, publicar y distribuir las Resoluciones Rectorales, de Consejo Universitario, así como de Asamblea Universitaria y tramitarlas a las instancias correspondientes.
- Verificar que las indicadas resoluciones se emitan sustentadas en informes técnicos y legales.
- Sistematizar la información derivada de los trámites gestionados ante la dependencia generando las acciones para la emisión de las resoluciones, informes, actas y otros que oportunamente se demanden.
- Llevar el Registro de Grados y Títulos que otorga la Universidad.
- Organizar, Mantener y conservar los documentos, registros, actas y archivos de la Universidad.
- Actúa como fedatario de la Universidad y con su firma certifica la autenticidad de los documentos oficiales emitidos por la Universidad.
- Administra el Archivo Central

- Supervisar, coordinar y controlar el normal funcionamiento de las unidades a su cargo.
- Otras funciones asignadas por el Rectorado.

Por lo tanto, se evidencia que SG realiza tratamiento de documentos que contienen datos personales, que el nivel de criticidad es alto y que es absolutamente necesario implementar controles de seguridad para el: a) Almacenamiento, copias y accesos a la documentación no automatizada; b) Trasladado de dicha documentación; c) Prestación de servicios sin accesos a datos personales. Según el Capítulo V "Medidas de Seguridad" del Reglamento de LPDP.

CAPÍTULO V: INGENIERÍA DE LA PROPUESTA.

5.1. Etapa 1: Diagnóstico del estado actual de las medidas de seguridad en base a la LPDP

Esta etapa constituye la elaboración de un diagnóstico de las áreas mediante una auditoría preliminar, tomando como base para la evaluación las medidas presentadas en la Ley de Protección de Datos Personales y los controles de la NTP-ISO/IEC 17799:2007, las cláusulas utilizadas a detalle se muestran en la tabla 5, este diagnóstico muestra mediante tablas de resultados y gráficos de barras el porcentaje alcanzado en cuanto a las medidas dictadas por la Ley.

Tabla 3
Dominios de la NTP-ISO/IEC 17799:2007 que se contemplaron en la evaluación realizada a las áreas

DOMINIO DE LA NTP	DIGETI	Secretaría General
5. Política de Seguridad.	X	X
6. Aspectos Organizativos para la Seguridad.	X	X

9. Seguridad física y del entorno	X	X
10. Gestión comunicación y operaciones	X	X
11. Control de Accesos	X	
13. Gestión de incidentes en la seguridad de la información		X
15. Cumplimiento	X	

Dentro de la Etapa 1 se trabajó en base a las actividades recomendadas para una auditoría por ISACA (Information Systems Audit and Control Association), las actividades son:

Planificar la Auditoría: En esta actividad se hizo la recolección de la información sobre las áreas de DIGETI y Secretaria General, esta información obtenida se analizó, para luego hacer la elaboración del Plan de Auditoría. El plan se puede apreciar en el anexo 1.

Este plan de auditoría contiene el alcance de la Auditoría, además que presenta el instrumento de evaluación, así como la guía ponderación y las técnicas de auditoría a utilizar.

En la siguiente tabla 6 y 7 se presenta las guías de ponderación establecidas dentro del plan de auditoría, aplicadas en las áreas de DIGETI y Secretaria General respectivamente.

Tabla 4
Guía de ponderación para la auditoría utilizada en DIGETI

Factores primarios	Peso x Factor	Valor Total
Medidas de Seguridad para el Tratamiento Lógico de Datos Personales		100 %

1. Seguridad para el tratamiento de la información Personal	30 %	
2. Conservación, respaldo y recuperación de los datos personales	25 %	
3. Transferencia Lógica o Electrónica de los Datos Personales	30 %	
4. Prestación de servicios sin acceso a datos personales	15 %	

Tabla 5
Guía de ponderación para la auditoría utilizada en Secretaría General

Factores primarios	Peso x Factor	Valor Total
Medidas de Seguridad para el Tratamiento Físico de Datos Personales		100 %
1. Almacenamiento, copia y acceso a la documentación no automatizada.	30 %	
2. Traslado de la documentación no automatizada.	25 %	
3. Prestación de servicios sin acceso a datos personales	30 %	

Con el resultado de esta primera actividad se realiza el plan de auditoría el cual presenta la siguiente información:

- Datos Generales de la Organización, así como una descripción de las principales actividades de la Organización y se presenta la misión y visión de la organización.
- Objetivos de la auditoría: Se describe el objetivo general de la auditoría, así como sus objetivos específicos; en este caso se encontraron 6 objetivos específicos que responden a las medidas presentadas por la Ley N° 29733.
- Descripción de la situación actual del área a evaluar, en el cual se detalla las actividades que desempeñan cada área, además que presenta la relación de los

puestos dentro del área y sus funciones, se describen las tecnologías de información actuales

- Aspectos de Evaluación donde se describe en base a que se está haciendo la evaluación, en este caso se describe los artículos del capítulo V de la Ley de Protección de Datos personales, las cláusulas de la NTP-ISO/IEC 17799:2007 que luego de hacer la evaluación serán de apoyo para implementar las medidas.
- El alcance de la auditoría es la evaluación del cumplimiento de los Artículos 39 al 46 del Reglamento de la Ley Nro. 29733, tomando como referencia para el cumplimiento los dominios 5, 6, 9, 10, 11, 13 y 15 de la NTP-ISO/IEC 17799:2007.
- Las limitaciones que son los aspectos no abarcados tanto de la ley, y las cláusulas de la NTP
- Las guías de ponderación de la auditoría presentan el peso de manera porcentual y el puntaje de cada pregunta a presentar en la evaluación.
- Guías de auditoría donde se describe las actividades que serán evaluadas, los procedimientos a realizar por los auditores, las herramientas utilizadas por los mismos, los recursos (materiales y herramientas), y las observaciones que debe tener el evaluador al momento de hacer la verificación de cada pregunta.
- El check list es la herramienta que se utilizó para la evaluación que consistió en 2 partes: Una evaluación de Medidas de Seguridad para el Tratamiento Lógico de Datos Personales (ver anexo 2) aplicada al área de DIGETI y una aplicada a Secretaria General sobre evaluación de Medidas de Seguridad para el Tratamiento Físico de Datos Personales (ver anexo 3) con un total de 57 y 29 preguntas respectivamente.

El plan de auditoría, así como el instrumento, fueron previamente validados por la Directora de la Oficina de Gestión de la Calidad de la UPeU y experta en materia de auditoría.

Ejecutar la Auditoría: En esta actividad se realizaron las acciones programadas en el plan de auditoría, se aplicaron los instrumentos y herramientas de evaluación. Se obtuvieron las evidencias y desviaciones.

Una vez realizado el plan de auditoría se hizo la respectiva presentación del documento a los jefes de cada área mediante una reunión en cada área, para así obtener la aprobación luego de hacer mínimas sugerencias u observaciones.

Luego de ser aprobado el plan de auditoría se procedió a realizar las actividades en las fechas del cronograma, según la guía de auditoría se organizó una reunión en el área con las personas interesadas.

Las evaluaciones se realizaron en las áreas de trabajo tanto de DIGETI como de Secretaria General, se reunieron con los responsables de las siguientes oficinas:

DIGETI: Área de Desarrollo, Redes y Conectividad, Mesa de Ayuda

Secretaria General: Archivo Institucional, Grados y Títulos, Oficina de trámite documentario.

Además, se hizo la toma de evidencias de las no conformidades encontradas durante la evaluación por medio de registro fotográfico en su mayoría, pruebas y testimonios orales.

Presentar Informe de la Auditoría:

Una vez terminada la evaluación con las listas de chequeo, se procedió a recoger la información para armar el documento de Dictamen de la Auditoría para presentar a las áreas involucradas y tengan conocimiento del nivel de cumplimiento de la LPDP.

Las no conformidades o desviaciones encontradas en el área de DIGETI fueron especificadas en el informe de dictamen, se procedió a sacar el puntaje alcanzado tal y como se muestra en la figura 17:

- **CONTROL: CONSERVACIÓN, RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.**

a) Evaluar el control de seguridad en los ambientes que contiene datos.

	VALOR	NO	PARCIAL	SI	TOTAL
2. Conservación, respaldo y recuperación de Datos Personales	25.0%				
2.1 Evaluar el control de seguridad en los ambientes que contienen datos	10.0%				
2.1.1 ¿Los perímetros del edificio o local que contienen los medios de almacenamiento de Información son físicamente solidos?	2.0%			x	2
2.1.2 ¿Las puertas y ventanas están protegidas de accesos no autorizados por mecanismos de control: Por ejemplo vallas, alarmas , relojes, etc.	2.0%			x	2
2.1.3 ¿Los medios de almacenamiento de Información se encuentran físicamente separados de aquellos ajenos a la organización?	2.0%		x		1
2.1.4 ¿Se usan controles de autenticación para restringir el acceso a los ambientes de procesamiento y almacenamiento de Información personal?	2.0%		x		1
2.1.5 EL personal de servicios de ajenos al área ¿cuenta con acceso restringido a las áreas seguras o los medios de procesamiento de Información Personal?	2.0%			x	2
TOTAL					**8.0**

Resultados: Total: 10.0 = 100%
Alcanzado: 8.0 = 80.0%

Figura 17. Conteo del puntaje obtenido en la evaluación en el punto 2 referente a la Conservación, respaldo y recuperación de datos personales en DIGETI (**Fuente:** Elaboración propia)

El desarrollo del conteo de los demás puntos de la evaluación tanto de DIGETI y de SG se encuentran dentro del Informe de Dictamen de Auditoría en el anexo 6.

Como resultados obtenidos de la evaluación para conocer el nivel de cumplimiento del Capítulo V “Medidas de Seguridad” del Reglamento de la Ley de Protección de Datos Personales fue el siguiente:

Sobre información personal dentro de un Banco de Datos Automatizado (Sistema Académico – DIGETI) el resultado obtenido se especifica en la siguiente tabla 8.

Tabla 6

Resultados de evaluación preliminar en DIGETI

Factores primarios	% TOTAL	% Alcanzado	Resultado Cualitativo
1. Seguridad para el tratamiento de la Información Digital	30 %	14 %	MEDIO
2. Conservación, respaldo y recuperación de los datos personales	25 %	18.8 %	BUENO
3. Transferencia Lógica o Electrónica de los Datos Personales	30 %	15.75%	MEDIO
4. Prestación de servicios sin acceso a datos personales	15 %	5.63%	MALO
TOTAL	**100 %**	**54.2 %**	**MEDIO**

Sobre información personal dentro de un Banco de Datos no Automatizado. (Archivo Académico Institucional – Secretaria General) el resultado obtenido se especifica en la siguiente tabla 9.

Tabla 7
Resultados de la evaluación preliminar en Secretaria General:

Factores primarios	% TOTAL	% Alcanzado	Resultado Cualitativo
1. Almacenamiento, copia y acceso a la documentación no automatizada.	50 %	29 .38%	MEDIO
2. Traslado de la documentación no automatizada.	30 %	12%	MEDIO
3. Prestación de servicio sin acceso a datos personales	20 %	2.5 %	BAJO
TOTAL	**100 %**	**43.88 %**	**MEDIO**

El resultado general de forma cualitativa y considerando los niveles de BAJO, MEDIO Y ALTO, vendría a ser **MEDIO-BAJO** en cuanto al cumplimiento de Medidas de Seguridad exigidas por la LPDP.

5.2. Etapa 2: Planificación de las mejoras en base a los controles de la NTP-ISO/IEC 17799:2007

La etapa 2 comprende las actividades como indica en la Figura 9, en cuanto a la planificación de la mejora; la primera actividad:

Actividad 1: Examinar los artículos de las "Medidas de Seguridad" de la LDPD:

En esta actividad se realizó un contraste de las no conformidades encontradas en la evaluación con los artículos del Reglamento de la Ley en una tabla indicando a cuál de ellas pertenece cada una. Se inició con las no conformidades concernientes a la seguridad para el tratamiento digital en las sub áreas de DIGETI, estas se aprecian en la tabla 10, 11, 12 y 13.

Tabla 8
Cuadro de no conformidades encontradas en el sub área de Desarrollo de Sistemas en cuando al Artículo 39 del Reglamento de la LPDP

Área evaluada	Artículo de la Ley	No conformidades
DIGETI	Artículo 39: Seguridad para el tratamiento de la información digital	• Inexistente función de bloqueo de usuario luego de 5 intentos de autenticación fallidos. • Inapropiados requisitos para la creación de contraseñas • Inexistente documento de los derechos de acceso a usuarios • Inexistente documento de entendimiento de las condiciones de acceso para los usuarios. • Inexistente registro formal de personas registradas al sistema • Deficiente eliminación y bloqueo de usuarios que dejan la organización • Inexistentes políticas para la disposición de privilegios. • Inexistente documentación sobre el proceso de autorización • Inexistente revisión de usuarios para evitar privilegios no autorizados.

		• Deficiente revisión en las asignaciones de privilegios y autorizaciones en usuarios con privilegios especiales. • Incompleta información en los reportes de acceso. • Inexistentes flujos de trabajo o procedimientos establecidos y documentados en la gestión de acceso. e Inadecuada realización de actividades de acuerdo a lo documentado. • No garantizada realización de auditorías para el control de accesos. • Inexistentes auditorías para el control de la Protección de Datos Personales.

Tabla 9

Cuadro de no conformidades encontradas en el sub área de Redes y Conectividad en cuando al Artículo 40 del Reglamento de la LPDP

Área evaluada	Artículo de la Ley	No conformidades
DIGETI	Artículo 40: Conservación, respaldo y recuperación de los datos personales	• Inadecuado lugar de almacenamiento de los medios de procesamiento de datos. • Deficiente control de autenticación para el control de acceso al área de procesamiento de Datos información. • Copias de respaldo sin técnicas de cifrado • Inadecuado lugar de almacenamiento físico de las copias de seguridad. • Inadecuadas medidas de seguridad física del ambiente que contiene copias de seguridad • Deficiente información de pruebas a las copias de respaldo.

Tabla 10

Cuadro de no conformidades encontradas en las sub áreas de Redes y Conectividad; y Dirección General en cuando al Artículo 40 del Reglamento de la LPDP

Área evaluada	Artículo de la Ley	No conformidades
	Artículo 41: Transferencia lógica o electrónica de datos personales	• Políticas inexistentes para la transferencia lógica de los datos personales. • Documentos inexistentes que garantice la transferencia nacional interna y externa de los datos personales. • Incumplimiento de políticas de transferencia que detallen los medios de transporte para cualquier tipo de transferencia de datos personales.

DIGETI	• Incumplimiento de políticas de transferencia que detallen los medios de transporte para cualquier tipo de transferencia de datos personales. • Software especializado inexistente para la transferencia de datos personales • No se encuentran establecidos los mecanismos de seguridad en las políticas. • No se garantiza la integridad y confidencialidad cuando la información lógica es transmitida • Incumplimiento de encriptación previo al envío • Inexistente evidencia del uso de técnicas para validar la identidad en los envíos digitales • El uso de herramientas de registro no autorizadas (Cámara de video, fotos, grabación, etc.) no están restringidos

Tabla 11

Cuadro de no conformidades encontradas en el sub área de Dirección General en cuando al Artículo 41 del Reglamento de la LPDP

Área evaluada	Artículo de la Ley	No conformidades
DIGETI	Artículo 46: Prestación de servicios sin acceso a datos personales.	• Inexistentes documentos o cláusulas contractuales que limiten los detalles de la prestación de servicios internos • Inexistentes documentos o cláusulas contractuales que limiten los detalles de la prestación de servicios externos • Inexistencia de compromisos de confidencialidad a los prestadores de servicios externos • No garantizada destrucción de la información al terminar un servicio con terceros externos.

De la misma manera se hizo el contraste de las no conformidades que están asociadas a los artículos del reglamento que hablan sobre la Seguridad para el tratamiento físico, estas no conformidades se aprecian en la tabla 14, 15 y 16.

Tabla 12

Cuadro de no conformidades respecto al Art. 41 de la LPDP

Área evaluada	Artículo	No Conformidades
Secretaria General	Artículo 42: Almacenamiento de la de documentación no automatizada	• Inapropiada separación de documentos que contienen datos personales para evitar su exposición • No garantizado proceso de autorización para generar o eliminar copias de documentos que contienen datos personales • Inexistente procedimiento de destrucción de documentos que garanticen la no recuperación • Inexistente documento que indique la responsabilidad ante algún incidente relacionado al acceso no autorizado a documentos que contienen datos personales • Deficiente procedimiento de autorización a los usuarios que deseen acceder a los documentos de datos personales • Inexistente documento de registro de los usuarios autorizados y no autorizados para el acceso al banco de datos • Inexistente documento de registro de personas que accedieron al banco de datos (Archivo Institucional)
	Artículo 42: Almacenamiento de la de documentación no automatizada	

Tabla 13

Cuadro de no conformidades respecto al Art. 43 de la LPDP

Área evaluada	Artículo	No Conformidades
Secretaria General	Artículo 43: Copia o reproducción Artículo 44: Acceso a la documentación Artículo 45: Traslado de la documentación no automatizada	• Inexistente documento de registro de los usuarios o mensajeros autorizados para trasladar la información con datos personales. • Inexistente mecanismo de verificación de no vulneración del contenedor en el cual se trasporta la información. • Inexistente registro de incidentes de seguridad relacionados a la gestión de los documentos que contienen datos personales • Inexistente procedimiento de comunicación al propietario de banco de datos luego de darse un incidente con datos personales.

Tabla 14

Cuadro de no conformidades respecto al Art. 46 de la LPDP

Área evaluada	Artículo	No Conformidades
Secretaria General	Artículo 46: Almacenamiento de la de documentación no automatizada.	• Inexistente documento de registro de los usuarios o mensajeros autorizados para trasladar la información con datos personales. • Inexistente mecanismo de verificación de no vulneración del contenedor en el cual se trasporta la información.

Actividad 2 y 3: Analizar y determinar los controles de la NTP-ISO/IEC 17799:2007 adecuados para la mejora:

Dentro de estas dos actividades se realizó el análisis de la NTP para poder determinar que controles se ajustaban a los requisitos que indican en el reglamente de la LPDP, para esto se hizo la siguiente tabla que muestra cada artículo del Reglamento en su Capítulo V y a su lado derecho los controles que se ajustan a dichos requisitos.

Tabla 15
Relación de los requisitos del Reglamento de la LPDP y su control adecuado

Nro. Artículo	**Requisitos**	**Control NTP-ISO/IEC 17799:2007**
Artículo 39	Control de accesos a la información de DP Gestión de accesos desde el registro de un usuario. Gestión de Privilegios. Identificación segura del usuario ante el sistema. Verificación periódica de privilegios. Procesos documentados de las actividades. Generar y mantener registros de interacción con el sistema. Establecer procedimientos de identificación y autentificación.	5. Políticas de seguridad de la Información 11.1 Requisitos de negocio para el control de accesos. 11.2 Gestión de accesos de Usuarios 11.3 Responsabilidades de los Usuarios.

Artículo 40	Controles de Seguridad Física. Procedimientos que contemplen la verificación de la integridad en los respaldos. Medidas que garanticen la recuperación completa ante una interrupción o daño.	9. Seguridad Física y del Entorno 10.5 Gestión de respaldo y recuperación.
Artículo 41	Documentación de autorización para transferencia lógica Contar con medios de transporte de información. Medidas de seguridad para el transporte de datos personales.	10.8 Intercambio de información. 12. Adquisición, desarrollo y mantenimiento de sistemas.
Artículo 42	Medidas de protección física de los almacenes o archivadores que contienen documentos físicos.	9. Seguridad Física y del Entorno

Nro. Artículo	**Requisitos**	**Control NTP-ISO/IEC 17799:2007**
Artículo 43	Tener control sobre la copia o reproducción de documentos que contiene datos personales.	5. Políticas de Seguridad 9. Seguridad Física y del Entorno
Artículo 44	Controlar el acceso a la documentación física, Contar con mecanismos de identificación a los documentos. Registro de personas	9. Seguridad Física y del Entorno 13. Gestión de incidentes en la Seguridad de la información
Artículo 45	Medidas que impidan el acceso o manipulación de la documentación en traslado.	10.8 Intercambio de información
Artículo 46	Controles para personas que prestan servicios al área. Cláusulas contractuales para proteger la información en los prestadores del servicio.	5. Políticas de Seguridad 6. Aspectos organizativos para la seguridad.

Actividad 4: Elaborar documentos de los controles a ejecutar

Una vez realizado el análisis y haber determinado los controles de la NTP que se tomarán como base y referencia, se precedió a hacer las propuestas en base a las no conformidades; los documentos fueron agruparon de acuerdo al área auditada ya que el

Reglamento de la LPDP abarca información automatizada (DIGETI) y no automatizada (Secretaría General).

Propuesta de controles de seguridad para el cumplimiento de la Ley nro. 29733 en el área de DIGETI.

Basado en los controles de la NTP-ISO/ IEC 17799:20007, el documento se estructura en dos partes, un Control de Seguridad General que es una política para el área como se muestra en la siguiente figura 18.

Código de propuesta: PD001	**Tipo**: Documento
Clausula: POLÍTICA DE SEGURIDAD	
Control: Documento de política de seguridad de la información.	
Alcance: La política general es aplicable a todo el personal de DIGETI y trabajadores de la UPeU que realicen labores directamente con el área, también, a los usuarios externos que presten o prestare servicios al área. Implicará las actividades relacionados al (o la): 1. Seguridad para el tratamiento información digital 2. Conservación, respaldo y recuperación de datos personales 3. Transferencia lógica o electrónica de datos personales 4. Prestación de servicios sin acceso a datos personales	
Solución: Implementar una política general de seguridad lógica en DIGETI, para dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos del negocio, leyes y regulaciones. La política reflejará en absoluto los controles propuestos de la investigación.	

Figura 18. Política de seguridad digital para la protección de datos (**Fuente**: Elaboración propia)

La segunda parte del documento son controles de seguridad específicos, que se hicieron en base a las no conformidades encontradas en la primera etapa de la investigación (evaluación previa).

Estos controles se clasificaron de acuerdo al artículo de la Ley al que corresponde cada no conformidad o registro de hallazgo.

1. Seguridad para el tratamiento de la Información Digital

1.1 Evaluar el control de acceso a la información

En la siguiente figura 19 se detalla la propuesta PD002, un procedimiento para la Gestión de usuarios y privilegios.

Código de hallazgo: RD001, RD002, RD003, RD006, RD007, RD008, RD009, RD010, RD011, RD012, RD013, RD014	**Código de propuesta**: PD002
Descripción del hallazgo: El personal de DIGETI realiza sus actividades empíricamente, mas no se tiene un proceso documentado que refleje las actividades, tareas y otros aspectos para medir el proceso de creación de usuarios y privilegios. Así mismo, no se tiene un cronograma con fechas definidas para la revisión de accesos y privilegios.	
Clausula: CONTROL DE ACCESOS	
Control: Política de control de accesos, Gestión de accesos de usuario, Gestión de contraseñas de usuario	**Tipo**: Proceso y Política
Alcance: El área de Desarrollo de Sistemas y Mesa de Ayuda trabajarán en conjunto para él y cumplimiento del Proceso de Gestión de Usuarios, su alcance será el uso de contraseñas para el Sistema Académico.	
Solución: El sub área de Mesa de Ayuda y Desarrollo de Sistemas trabajarán en conjunto para el desarrollo y cumplimiento de la política, considerando a las áreas y/o alumnos de la universidad que soliciten del servicio. La política y el documento abarcarán únicamente el Sistema Académico. Incluye: ✓ Implementar un procedimiento formal para estandarizar una correcta autorización de privilegios al Sistema Académico, identificando los pasos que se debe seguir para ejecutar las solicitudes (Anexo 02); y realizar periódicamente revisión de los accesos y privilegios otorgados (Anexo 02). ✓ Directriz de contraseñas seguras (Anexo 03)	

Figura 19. Propuesta de un procedimiento para la Gestión de usuarios y privilegios (**Fuente**: Elaboración propia)

En esta figura 20 se describe la propuesta PD003, un formato para los derechos de acceso.

Código de hallazgo: RD004, RD005	**Código de propuesta**: PD003
Descripción del hallazgo: El sub área de Mesa de Ayuda realiza la creación de los usuarios al portal sea presencial o no, pero no indica al usuario que accesos se le está otorgando y obtener su entendimiento.	
Clausula: CONTROL DE ACCESOS	
Control: Política de control de accesos, Registro de usuarios	**Tipo**: Formato
Alcance: Su alcance es sólo en la creación de usuarios para el portal académico. Incluirá el formato físico o mensaje por correo electrónico según sea el caso.	
Solución: Se implementará un formato de los derechos de acceso que tendrá el usuario y una firma manifestando su entendimiento.	
Documento adjunto: Ver el Anexo 04 para el formato de derechos de acceso.	

Figura 20. Propuesta de formato de derechos de acceso (**Fuente**: Elaboración propia)

1.2 Evaluar una correcta gestión de privilegios.

La propuesta para este apartado de ley y como solución a las no conformidades: RD009, RD011, RD012, RD013, RD014 relacionados a la gestión de privilegios se encuentra implícito en la PD002.

1.3 Evaluar los reportes de accesos.

Debido al cumplimiento parcial de estos apartados de la evaluación la propuesta se encuentra dentro del documento de recomendaciones del anexo 15 de la propuesta.

1.4 Evaluar la realización del procedimiento documentado.

La propuesta a las no conformidades RD016 y RD017 de este apartado referente a que debe tener un proceso documentado viene a ser la PD002 descrito en la Figura 21. En cuanto al RD018 se hizo la siguiente propuesta:

Código de hallazgo: RD018	**Código de propuesta**: PD004
Descripción del hallazgo: Ausencia de realización de auditorías para verificar el cumplimiento del proceso de control de accesos	
Clausula: CUMPLIMIENTO	
Control: Registro de la auditoría	**Tipo**: Cronograma (registro)
Alcance: Su alcance es sobre el cumplimiento del proceso de Gestión de usuarios y privilegios	
Solución: Desarrollar un programa anual que refleje las fechas específicas, y el responsable para realizar una evaluación de cumplimiento del proceso de control de accesos.	

Figura 21. Propuesta del cronograma de auditoría en el control de accesos (**Fuente**: Elaboración propia)

2. Conservación, respaldo y recuperación de datos personales.

2.1 Evaluar el control de seguridad en los ambientes que contienen datos.

En la siguiente figura 22 se aprecia la propuesta PD005, una política para el respaldo y recuperación para DIGETI.

Código de hallazgo: RD019, RD022, RD023, RD024	**Código de propuesta**: PD005
Descripción del hallazgo: DIGETI realiza back ups continuamente pero no se realiza un registro de cada acción realizada. También, mantiene una copia de otra organización perteneciente a la red, pero sin ningún contrato por medio. Así mismo, mantiene una réplica dentro de una zona geográfica no permitida.	
Clausula: GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Control: Gestión de respaldo y recuperación	**Tipo**: Política específica y Formato
Alcance: El alcance de la política es sobre las labores que realiza el sub área de Redes y Conectividad sobre el "Centro de datos" y, los mismos que serán los responsables de velar por el cumplimiento de la política y el formato.	
Solución: Implementar una **política** específica y un **formato** que contemple las medidas y requisitos que se deberán tomar los encargados de DIGETI al realizar respaldos y la recuperación de la misma.	

Figura 22. Propuesta de políticas para el respaldo y la recuperación (**Fuente**: Elaboración propia)

En la figura 23 se describe la propuesta PD006, con el fin de reforzar la autentificación al Centro de Datos.

Código de Hallazgo: RD020	**Código de Propuesta**: PD006
Descripción del hallazgo: Existe un control de seguridad en el centro de datos, pero actualmente tiene algunas deficiencias con el carnet, puerta y alarma.	
Clausula: SEGURIDAD FISICA Y DEL ENTORNO	
Control: Perímetro de seguridad física y Controles físicos de entradas	**Tipo**: Tecnología
Alcance: El aseguramiento de autentificación se realizará en el Centro de Datos de DIGETI. El encargado de la implementación será una empresa tercera pero el responsable o responsables de controlar los accesos serán los trabajadores del sub área de Redes y Conectividad según la política de control físico.	
Solución: Mejorar el control de autentificación para autorizar y validar el acceso (visitas) al Centro de Datos. Renovar las alarmas, rejas u otros controles de acceso físico al Centro de Datos.	

Figura 23. Propuesta para el aseguramiento de la autentificación al Centro de Datos (**Fuente**: Elaboración propia)

2.2 Evaluar los mecanismos de respaldo de la información

La propuesta para el RD021 que evidencias la ausencia de técnicas de cifrado para proteger las copias de respaldo de los datos personales se encuentran en el documento de recomendaciones de la propuesta general.

2.3 Evaluar procedimientos de restauración de respaldos:

El control a implementar para cumplir este apartado se encuentra en la propuesta PD005 mostrado en la figura del documento de propuesta para DIGETI.

3. Transferencia lógica o electrónica de datos personales

3.1 Supervisar la autorización del titular del banco de datos personal (BDP) para la transferencia.

Para los registros de hallazgos evidenciados en la figura 24, se muestra la propuesta de una política de transferencia lógica para la protección de datos.

Código de hallazgo: RD025, RD026, RD027, RD028, RD029, RD030	**Código de propuesta**: PD007
Descripción del hallazgo: Actualmente DIGETI tiene deficiencias al momento de autorizar la transferencia de datos por el encargado del banco de datos. Así mismo al momento de garantizar y evidenciar la confidencialidad e integridad en la transferencia lógica de datos con alguna organización externa.	
Clausula: GESTIÓN DE COMUNICACIONES Y OPERACIONES Y ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
Control: Intercambio de información, Servicios de correo electrónico y Política de uso de los controles criptográficos	**Tipo**: Política específica
Alcance: La política será aplicable a las sub áreas de Desarrollo Académico y Redes y conectividad bajo su responsabilidad. El Director de DIGETI como Encargado del Banco de Datos evaluará y autorizará la transferencia (nacional e internacional).	
Solución: Implementar una **política** específica que señale la obligación y necesidad de obtener la autorización para las transferencias, los mecanismos adecuados para garantizar la seguridad durante la transferencia (nacional e internacional), así mismo reflejará la necesidad de registrar la transferencia exitosa y el uso de los medios de transferencia permitidos. Desarrollar formato modelo para la autorización de transferencias.	

Figura 24. Propuesta de política de transferencia lógica de datos (**Fuente**: Elaboración propia)

3.2 Medios de transporte para la transferencia de datos personales.

Para los siguientes hallazgos, RD028, RD029, RD030, que tratan sobre la ausencia de medios de transportes autorizados por el titular de BD se propone el PD007 mostrado en la figura 24.

Por otro lado, el hallazgo con código RD031 que pide el uso de un software especializado para trasferencia de información que contienen datos personales, se especificó una propuesta en el documento de recomendaciones del anexo 15 de la propuesta de controles.

3.3 Mecanismos de seguridad en la transferencia de datos personales.

La propuesta del hallazgo con código: RD032 sugiere obtener algún soporte informático que permita enviar datos encriptados y que asegure la integridad de estos.

4. Prestación de servicios sin acceso a datos personales.

4.1 Servicios internos de la organización o área sin acceso a datos personales.

En el caso de controles que ayuden a mejorar el resguardo de la integridad en la información en ambientes donde se realicen labores con terceros que prestan servicios al área de DIGETI, solo se pueden aplicar políticas internas, ya que DIGETI no se encarga de hacer las contrataciones de forma directa.

La siguiente figura 25 propone contar con una política para el control físico, teniendo como enfoque limitar el acceso al personal, realización de trabajos y el uso de equipos de registro.

<table>
<tr><td>Código de hallazgo: RD033, RD034</td><td>Código de propuesta: PD008</td></tr>
<tr><td colspan="2">Descripción del hallazgo: Actualmente en DIGETI no existe un documento que límite la realización de trabajos y el acceso de personal interno (UPeU) al área o externo sea otra organización respecto al centro de datos.</td></tr>
<tr><td colspan="2">Clausula: SEGURIDAD FÍSICA Y DEL ENTORNO, ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD</td></tr>
<tr><td>Control: Controles físicos de entradas, Seguridad en los accesos de terceras partes</td><td>Tipo: Política</td></tr>
<tr><td colspan="2">Alcance: La política será al nivel de área (política específica). El personal de DIGETI, externos a la organización y demás áreas de la UPeU que deseen acceder al área de datos deberán cumplir la política.</td></tr>
<tr><td colspan="2">Solución: Implementar una política específica donde señale detalladamente quienes son las personas autorizadas al área de datos. Se supervisará y monitoreará las visitas al Área de Datos. El documento cumplirá con lo siguiente:

• Limitar el acceso del personal ajeno al área a documentos que contengan datos personales.
• Limitar la realización de trabajos que no impliquen el tratamiento de datos personales.
• Restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de datos, salvo autorización del titular del banco de datos personales o encargado.</td></tr>
</table>

Figura 25. Propuesta de una política específica de control físico (**Fuente**: Elaboración propia)

4.2 Servicios externos a la organización sin acceso a datos personales.

En el caso de los servicios externos a la UPeU prestados al área de DIGETI, se propuso un tipo de cláusula contractual que será evaluada por las áreas encargadas de hacer los contratos para la prestación de servicios a la organización.

La siguiente figura 26 muestra aprobar un instructivo para la gestión de acuerdos en DIGETI. Posteriormente la figura 27 propone un acuerdo de confidencialidad que tiene que ser entendido y firmado por los trabajadores del área comprometida.

Código de hallazgo: RD035, RD036, RD037, RD038, RD039	**Código de propuesta**: PD009
Descripción del hallazgo: Actualmente no se gestiona la seguridad en la contratación de servicios externos. Teniendo en cuenta la labor que realizaran por medio de cláusulas contractuales o documentos que respalden su seguridad.	
Clausula: GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Control: Gestión de servicios externos	**Tipo**: Política
Alcance: La Dirección de DIGETI y el personal encargado de gestionar los servicios deberá considerar la instrucción al momento de contratar algún servicio externo donde traten de datos personales.	
Solución: Implementar una instrucción para una correcta gestión de servicios (contractuales y/o legales) donde los terceros que presten servicios a la UPeU por encargo de DIGETI, estén enterados de sus obligaciones y responsabilidades que implique acceder, procesar, comunicar o manejar la información de la organización.	

Figura 26. Propuesta de instrucción para la gestión de acuerdos (**Fuente**: Elaboración propia)

Código de hallazgo: RD037	**Código de propuesta**: PD010
Descripción de hallazgo: El personal interno de DIGETI no cuenta con un documento donde describa la confidencialidad que deberá guardar durante la prestación de sus servicios. El personal realiza sus labores sin declarar el compromiso que tendrá al tratar con información sensible.	
Clausula: ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Acuerdos de confidencialidad	**Tipo**: Documento
Alcance: El documento de acuerdo de confidencialidad será firmado por el personal de DIGETI, otorgando de esa manera la comprensión del acuerdo y su compromiso.	
Solución: Implementar un documento contractual para los empleados de DIGETI donde acepten y firmen los términos y condiciones del contrato del empleo. El documento también considerará las responsabilidades, derechos y las acciones que se ha de tomar en caso incumpla el acuerdo durante el periodo de tiempo definido.	

Figura 27. Propuesta del acuerdo de confidencialidad (**Fuente**: Elaboración propia)

Como se mencionó anteriormente, las propuestas se dividieron en 2 partes de acuerdo a las áreas en las que se hizo la evaluación por lo cual las propuestas para Secretaria General fueron las siguientes:

A. Control de Seguridad General:

La siguiente figura 28 muestra el documento propuesto como política general, donde engloba los controles específicos descritos posteriormente.

Código de propuesta: PS001	**Tipo**: Documento
Clausula: POLÍTICA DE SEGURIDAD	
Control: Documento de política de seguridad de la información.	
Alcance: La política general es aplicable a todo el personal de Secretaría General y trabajadores de la UPeU que realicen labores directamente con el área, también, a los usuarios externos que presten o prestare servicios al área. Implicará las actividades relacionados al (o la): 1. Almacenamiento, copia y acceso a la documentación no automatizada 2. Traslado de documentación no automatizada 3. Prestación de servicios sin acceso a datos personales	
Solución: Implementar una política general de seguridad física en Secretaría General, para dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos del negocio, leyes y regulaciones. La política reflejará en absoluto los controles propuestos de la investigación.	

Figura 28. Propuesta de política de seguridad física para la protección de datos (**Fuente**: Elaboración propia)

B. Control de seguridad específico:

Realizado en base a los controles de la NTP para combatir las no conformidades obtenidas en la evaluación previa

1. Almacenamiento, copia y acceso a documentación no automatizada.

1.1 Almacenamiento de documentación no automatizada: Se logró conocer que la organización cumple con los requisitos de la NTP-ISO/IEC 17799:2007, sin embargo, para seguir manteniendo el nivel y mejorarlo en el tiempo se propone una serie de recomendaciones descritas en el documento de recomendaciones anexo 2 de la propuesta.

1.2 Copia y reproducción de la documentación no automatizada: La propuesta para este indicador radica en la aplicación de un documento que indique las responsabilidades de cada trabajador del área que está en constante trabajo con documentación física que contengan datos personales como se puede ver en la siguiente figura 29.

Código de hallazgo: RS001	**Código de propuesta**: PS002
Descripción del hallazgo: Los trabajadores conocen sus responsabilidades por l experiencia en el puesto o alguna capacitación de su predecesor, mas no existe u documento que señale aquellas actividades encargadas y su negativa al incumplirlo.	
Clausula: ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Asignación de responsabilidades sobre seguridad de la información	**Tipo**: Documento
Alcance: El documento abarcará el personal en absoluto de Secretaria General. Señalará las funciones respecto a la seguridad física, el área se encargará de completar con las funciones propias al área.	
Solución: Implementar un documento que contenga el responsable, aprobador, consultado e informado de cada actividad perteneciente a Secretaría General, identificando claramente el activo o proceso que deberá velar y el efecto de incumplirla.	

Figura 29. Propuesta de la matriz de asignación de responsabilidades (RACI) (**Fuente**: Elaboración propia)

Otro indicador de este apartado relacionado a la seguridad en la copia y reproducción de información física, fue contar con un debido proceso de destrucción de las copias de documentación fallida u obsoleta.

La siguiente figura 30 propone implementar un procedimiento formal para la destrucción de documentos y adquirir una maquina destructora de papel.

Código de hallazgo: RS002	**Código de propuesta**: PS003
Descripción del hallazgo: Los documentos inválidos son almacenados en un lugar con fácil acceso. No se realiza una evaluación previa para ser reciclado.	
Clausula: GESTIÓN DE COMUNICACIÓN Y OPERACIONES	
Control: Eliminación de medios	**Tipo**: Tecnología y Procedimiento
Alcance: La máquina trituradora permanecerá en lugar determinado y su uso permitirá la eliminación de documentos de toda el área de Secretaria General. Existirá un responsable de dicha tarea.	
Solución: Implementar un procedimiento que indique los responsables de la actividad, evitando destrucciones no planificadas y minimizando el riesgo de filtro de información sensible a personas externas con la eliminación segura. Adquirir una maquina destructora/trituradora de papel, para eliminar documentos de forma segura y sin peligro cuando no se necesiten más. Implementar un Registro de control de documentos a destruir para mantener la trazabilidad de los documentos que inicien con el procedimiento.	

Figura 30. Propuesta para la destrucción planificada de documentos (**Fuente**: Elaboración propia)

1.3 Acceso a la documentación no automatizada: Las no conformidades pertenecientes a esta sub categorías están relacionados a la propuesta PR002 ya que se detallarán las responsabilidades de cada trabajador o puesto de labor.

Otra propuesta para mejorar fue la siguiente que mejora nivel ya que se seguirá un protocolo de autorización y registro de accesos al banco de datos. Ver figura 31.

Código de hallazgo: RS004, RS005, RS006 (Respectivamente).	**Código de propuesta**: PS004
Descripción del hallazgo: Los usuarios con acceso al área de datos no son autorizados por el encargado o titular del banco de datos mediante un documento de registro. Tampoco existe trazabilidad en los accesos al área de datos.	
Clausula: GESTIÓN DE COMUNICACIÓN Y OPERACIONES	
Control: Segregación de tareas	**Tipo**: Documento
Alcance: El documento se autorizará y registrará en el área de Secretaría General, sin embargo, los usuarios registrados y autorizados pueden implicar trabajadores externos al área y a la UPeU.	
Solución: Separar las tareas y áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional. El Secretario General como Encargado del Banco de Datos autorizará tales segregaciones. Los documentos a implementar serán los siguientes: • Formato para la autorizar o retirar el acceso de usuarios al área de datos. • Formato para registrar la lista de usuarios autorizados a los datos personales. • Formato para mantener la trazabilidad del acceso al área de datos (persona, fecha, motivo, etc.)	

Figura 31. Propuesta de autorización y registro de accesos (**Fuente**: Elaboración propia)

2. Traslado de documentación no automatizada.

2.1 Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado.

Para asegurar un correcto proceso de traslado de documentación se propuso una serie de documentos para ejercer una mejor gestión., las especificaciones de estos documentos se los pueden observar en la figura 32.

Código de hallazgo: RS007, RS008, RS009, RS010 Y RS011 (Respectivamente).	**Código de propuesta**: PS005
Descripción del hallazgo: No existe un registro de las autorizaciones de traslado de documentos encargado por un responsable (Secretario General). Así mismo, no hay un registro para los usuarios y mensajeros autorizados a trasladar y su trazabilidad para el envió. Sabiendo que en su mayoría la información que trata Secretaría General es sensible, no se cuenta con mecanismo adicional de seguridad para su traslado.	
Clausula: GESTIÓN DE COMUNICACIÓN Y OPERACIONES	
Control: Medios físicos en tránsito	**Tipo**: Documento
Alcance: Los controles propuestos solo se usarán en el área de Secretaría General. El sobre para la transferencia de documentos sensibles no podrá ser usado para otras finalidades.	
Solución: Implementar documentos y procedimientos para proteger los medios contra personal no autorizado, mal uso o corrupción durante el transporte de los documentos de Secretaría General. Los documentos serán los siguientes: • Formato de una solicitud para la autorización del traslado de documentos que contengan datos personales, aprobado por el encargado o titular del banco de datos. • Formato para el registro de usuarios y/o mensajeros autorizados o no para trasladar datos personales. • Formato para mantener la trazabilidad ante usuarios y/o mensajeros autorizados para trasladar. • Implementar una política específica para el traslado de documentos.	

Figura 32. Propuesta para el aseguramiento del traslado de documentos (**Fuente**: Elaboración propia)

2.2 Eventos o incidentes en el traslado de documentos con datos personales.

La propuesta para tener una mejor gestión de incidentes fue en primer lugar hacer un procedimiento formal de las actividades a realizar como respuesta a un incidente que involucre información personal, además de contar con documentos que evidencien el seguimiento y la solución que se dio para estos casos. Ver figura 33.

Código de hallazgo: RS012, RS013, RS014 (Respectivamente).	**Código de propuesta**: PS006
Descripción del hallazgo: Durante las tareas comunes en el área, suceden incidentes de seguridad (Área de datos). Al ocurrir estos eventos, no existe un documento formal que facilite la respuesta a los incidentes. De la misma forma, estos eventos no suelen ser registrados ni notificados a la administración o al titular de los datos personales.	
Clausula: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
Control: Reportando los eventos en la seguridad de información	**Tipo**: Procedimiento y Documento
Alcance: La extensión del reporte de eventos y su respuesta abarcará el área de Secretaría General, la administración y la persona afectada directamente.	
Solución: Implementar un procedimiento de reporte de eventos junto con una respuesta a incidentes, estableciendo las acciones y los responsables que Secretaría General deberá tomar en cuenta al recibir dicho reporte. Los procedimientos y documento son los siguientes: • Formato para el registro y respuesta de los incidentes de seguridad relacionada al acceso o manipulación en el traslado. • Procedimiento para la notificación (en caso lo requiera) a la gerencia. • Procedimiento para la notificación al titular o titulares de los datos personales.	

Figura 33. Propuesta para lo notificación y respuesta a incidentes (**Fuente**: Elaboración propia)

3. Prestación de servicios sin acceso a datos personales.

3.1 Servicios internos de la organización o área sin acceso a datos personales.

En este caso Secretaría General al igual que DIGETI no realiza la contratación de personal que preste servicios directamente, por lo cual la propuesta debe ser implementada para otra área (Servicios, Mantenimiento), pero como recomendación se propuso contar con políticas internas como se pueden ver en la figura 33.

En cuanto a servicios de terceros ajenos a la institución, la contratación es por medio del área de mantenimiento o infraestructura dependiendo el alcance de la necesidad por lo cual la propuesta quedó en un documento de confidencialidad que debe ser firmado al iniciar las labores. Véase en la figura 33.

Actividad 5: Elaborar Documentos de trabajo.

Una vez concluidas las propuestas se procedió a elaborar los documentos de trabajo: políticas, documentos, formatos, etc. Para esto como ya se mencionó se tomaron en cuenta las recomendaciones y especificaciones de la NTP, así como la Directiva de Seguridad que brinda la ANPDP. A continuación, se mostrarán los documentos por cada propuesta hecha en la actividad anterior:

- PD001: Política de seguridad general (información digital)
- PD002: Proceso de Gestión de usuarios y privilegios
- PD003: Formato de derechos de acceso
- PD004: Cronograma de auditoría en el control de accesos.
- PD005: Política para el respaldo y recuperación
- PD006: Aseguramiento de autentificación al Centro de Datos
- PD007: Política de transferencia lógica de datos
- PD008: Política específica para el control físico
- PD009: Instrucción para la gestión de acuerdos
- PD010: Acuerdo de confidencialidad
- PS001: Política de seguridad general (información física)
- PS002: Matriz de asignación de responsabilidades (RACI)
- PS003: Destrucción planificada de documentos
- PS004: Autorización y registro de accesos
- PS005: Aseguramiento en el traslado de documentos
- PS006: Notificación y respuesta ante incidentes

5.3. Etapa 3: Ejecución de controles para la mejora de “medidas de seguridad”

La etapa 3 o la etapa de ejecución de los controles fueron planificadas para ser realizada en 4 etapas las cuales comprenden:

Actividad 1: Presentar los controles de seguridad a la dirección

La ejecución de esta actividad constó de la planificación de una reunión con las áreas de DIGETI y Secretaria General en sus respectivas oficinas:

En el caso de Secretaría General, se contó con la presencia del Secretario General y el Asistente de Estadística y TI a los cuales se les hizo la presentación de las propuestas desarrolladas en base a las no conformidades del dictamen de auditoría.

Para el área de DIGETI se acordó una reunión con su Director, así como con la coordinadora de Desarrollo de Sistemas, quien es la encargada del Sistema Académico, a cada uno de ellos, se les expuso las propuestas juntamente con los documentos respectivos.

Como resultado de esta actividad tenemos las actas de reuniones y un registro fotográfico presentado, ver el anexo 7 y 8 respectivamente.

Una vez presentados los controles a los jefes de área en la reunión se procedió a realizar el análisis de las propuestas para realizar alguna observación o recomendación por parte de ellos.

Actividad 2: Acordar controles necesarios a implementar

Al terminar el análisis y subsanando las observaciones obtenidas se realizó una reunión para poder obtener la aprobación de los controles a implementar que dio como resultado la siguiente tabla 18.

Tabla 16
Balance general de las políticas presentadas y aprobadas para la protección de Datos Personales

Área	DIGETI	Secretaria General
Nro. Controles propuestos	10	9
Nro. Controles aprobados	10	7
Nro. de Controles no aprobados	0	2

Como se observa en la tabla 18, al área de DIGETI se hizo la propuesta de 9 Controles Específicos y 1 Control general y se obtuvo la aprobación de los 10 por parte de la dirección, como se puede observar en la figura 34 que muestra el documento con las firmas de los encargados que aceptaron las propuestas para ser aplicadas en sus áreas.

UNIVERSIDAD PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

Propuesta de controles de seguridad para el cumplimiento de la Ley nro. 29733 en el área de Dirección General de Tecnologías de Información (DIGETI)

Equipo implementador	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Lima, Enero del 2018

Figura 34. Propuesta de controles de seguridad aprobados en el área de DIGETI (**Fuente:** Elaboración propia)

En cuanto al área de Secretaria General de los 9 controles se obtuvo la aprobación de 7 de ellos como se puede observar en la figura 35, el motivo por el cual no se aprobaron las propuestas PD007 y PD008, relacionadas a la implementación de políticas y cláusulas contractuales a la hora de obtener servicios de terceros ya sea personal interno y ajeno a la institución, es que el área no hace contratación directamente sino que es un área de apoyo

de la universidad la encargada de obtener estos servicios, por lo cual la propuesta debe evaluarse a un grado administrativo mayor.

UNIVERSIDAD
PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

Propuesta de controles de seguridad para el cumplimiento de la Ley nro. 29733 en el área de Secretaría General

Equipo implementador	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Secretaría General

Lima, Mayo del 2017

Figura 35. Propuesta de controles de seguridad en Secretaría General aprobada. (**Fuente:** Elaboración propia)

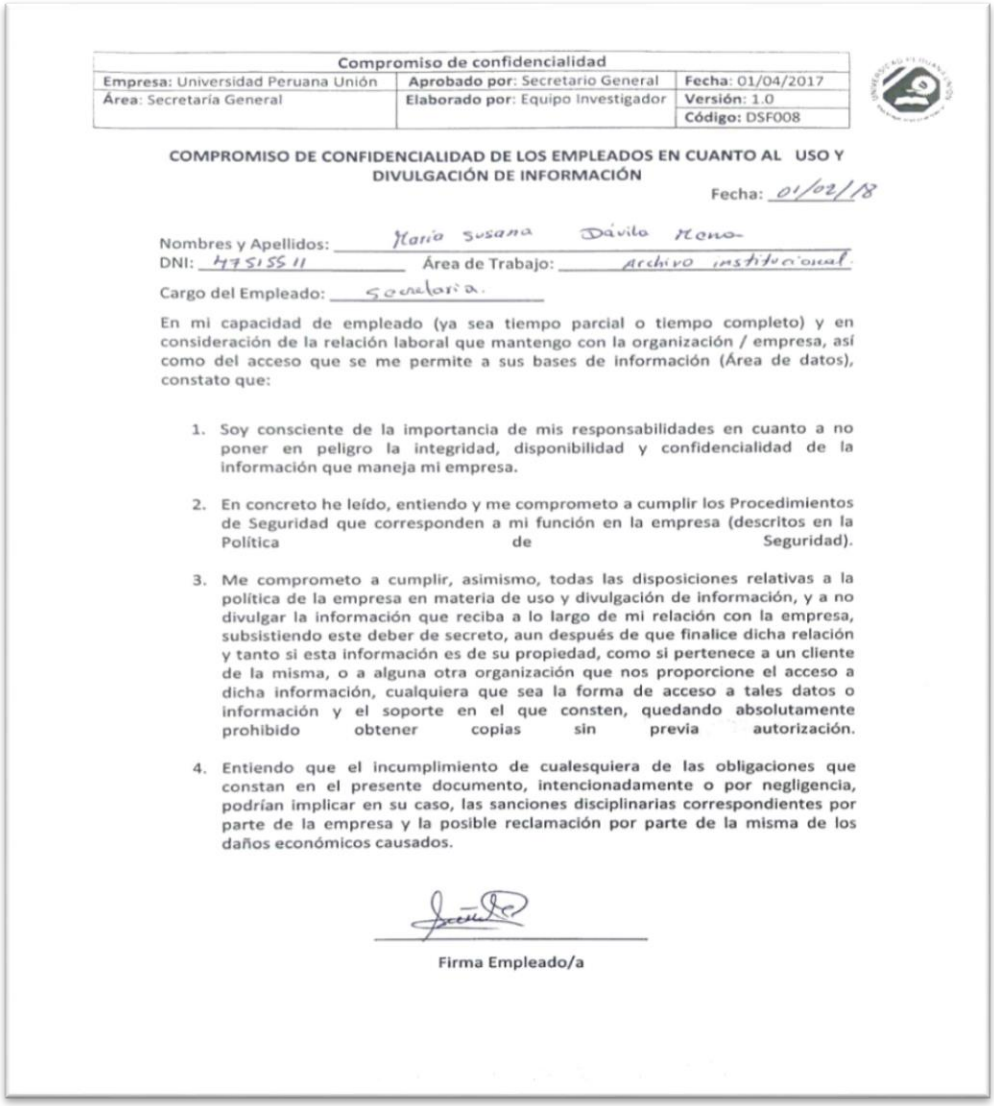
La implementación inició cuando el jefe del área aceptó y firmó los documentos presentados en la reunión, pero para hacerlo del conocimiento de los otros trabajadores del área se planificó dos reuniones que se detallan en la siguiente actividad.

Actividad 3. Concientizar personas interesadas.

Para esta actividad se coordinaron 2 sesiones generales en el caso de Secretaria General para poder compartir con todo el personal, las nuevas políticas que se habían implementado para el control de acceso al área de Archivo Académico Institucional, el proceso de Notificación de Incidentes, las políticas para el transporte de información fuera de la universidad, el proceso de destrucción de copias de documentos, etc.

También, se firmó el acta de cada reunión respectiva, como se muestra en el anexo 13.

En la segunda sesión general para el área de Secretaria General se hizo una socialización por áreas de los documentos a utilizar por cada oficina, donde se firmó el acuerdo de confidencialidad por cada trabajador (véase figura 36) para así cumplir con los estándares



Compromiso de confidencialidad		
Empresa: Universidad Peruana Unión	**Aprobado por:** Secretario General	**Fecha:** 01/04/2017
Área: Secretaría General	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: DSF008

COMPROMISO DE CONFIDENCIALIDAD DE LOS EMPLEADOS EN CUANTO AL USO Y DIVULGACIÓN DE INFORMACIÓN

Fecha: 01/02/18

Nombres y Apellidos: María Susana Dávila Mena
DNI: 47515511 Área de Trabajo: Archivo institucional
Cargo del Empleado: Secretaria.

En mi capacidad de empleado (ya sea tiempo parcial o tiempo completo) y en consideración de la relación laboral que mantengo con la organización / empresa, así como del acceso que se me permite a sus bases de información (Área de datos), constato que:

1. Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja mi empresa.
2. En concreto he leído, entiendo y me comprometo a cumplir los Procedimientos de Seguridad que corresponden a mi función en la empresa (descritos en la Política de Seguridad).
3. Me comprometo a cumplir, asimismo, todas las disposiciones relativas a la política de la empresa en materia de uso y divulgación de información, y a no divulgar la información que reciba a lo largo de mi relación con la empresa, subsistiendo este deber de secreto, aun después de que finalice dicha relación y tanto si esta información es de su propiedad, como si pertenece a un cliente de la misma, o a alguna otra organización que nos proporcione el acceso a dicha información, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.
4. Entiendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empresa y la posible reclamación por parte de la misma de los daños económicos causados.

Firma Empleado/a

Figura 36. Propuesta de controles de seguridad en Secretaria General aprobada. (**Fuente:** Elaboración propia)

En el área de DIGETI, se realizó una serie de visitas por cada sub área, en el caso de Oficina de Desarrollo de Sistemas, se presentó el procedimiento de Gestión de Usuarios y Privilegios (ver anexo 8), socializándolo y realizando una simulación de las actividades presentadas en dicho procedimiento, a su vez las nuevas políticas para DIGETI y el cronograma de auditorías para tener una mejor gestión de privilegios.

En la oficina de Redes y Conectividad, se presentaron los documentos que servirán para el control de visitas al Data Center, el formato para el control de backups y las políticas ya mencionados.

Con la Dirección del DIGETI se compartieron los documentos de autorización que deben de usarse cuando se necesite hacer alguna transferencia de datos a entidades externas.

Adicional a esto, se puede visualizar en los anexos las imágenes de la implementación.

5.4. Etapa 4: Evaluar resultados

Una vez realizada la implementación como etapa 4 de nuestra metodología está realizar una evaluación para ver los resultados post implementación. La planificación de la evaluación que fue hecha en la primera etapa sirvió como guía para esta última ya que se pretendió conocer si hubo alguna mejora en cuanto a los controles; así que el único cambio en la planificación de la evaluación es las fechas de aplicación.

La evaluación a DIGETI fue por oficinas, iniciando por Desarrollo de Sistemas, para evaluar, el indicador 1 “Seguridad para el tratamiento de la Información Digital” el cual demostró los siguientes resultados mostrados más a detalle en la Figura 37.

	VALOR	NO	PARCIAL	SI	TOTAL
1. Seguridad para el tratamiento de la Información Digital	**30.0%**				
1.1. Evaluar el control de acceso a la información	14.0%				0
1.1.1. ¿El Sistema Académico está protegido contra el acceso lógico no autorizado?	1.5%			x	1.5
1.1.2. ¿Se utilizan ID's únicos para dar acceso a los usuarios del Sistema Académico?	0.5%			x	0.5
1.1.3. ¿El servidor del sistema almacena contraseñas de inicio de sesión de manera cifrada?	1.0%			x	1
1.1.4. ¿Se permite que el usuario cambie la contraseña cuando lo desee?	0.5%			x	0.5
1.1.5. Para la creación de un nuevo usuario (Alumnos, Docentes, Administrativos)¿se revisa que el usuario tenga la autorización dada por el propietario del banco de datos?	1.0%			x	1
1.1.6. ¿Se requiere que las contraseñas contengan al menos 8 dígitos, números y al menos incluyan un carácter especial?	1.0%		x		0.5
1.1.7. Para la creación de un nuevo usuario (Alumnos, docentes, administrativos): ¿Revisa que el nivel otorgado sea apropiado para el propósito?	1.0%			x	1
1.1.8. Durante la creación de un nuevo usuario: ¿Se le proporciona a los usuarios un documento escrito de sus derechos de acceso?	1.0%		x		0.5
1.1.9. Para la creación de un nuevo usuario: ¿Se requiere a los usuarios la firma de un documento indicando el entendimiento de las condiciones de acceso?	1.0%			x	1
1.1.10. ¿DIGETI, se asegura que no se proporcione el acceso hasta haber completado los procedimientos de autorización?	1.0%			x	1
1.1.11. ¿Se mantiene un registro formal de todas las personas registradas para usar el servicio?	1.0%		x		0.5
1.1.12. ¿Se verifica la eliminación o bloqueo inmediato de los derechos de acceso a los usuarios que han cambiado de puesto o han dejado la organización?	1.5%			x	1.5
1.1.13. ¿Se asegura que no se emitan ID's redundantes a otros usuarios?	1.0%		x		0.5
1.1.14. ¿Se realiza un chequeo periódico para eliminar o bloquear los ID's de usuario o cuentas redundantes?	1.0%			x	1
TOTAL	14.0%				12.00
1.2. Evaluar una correcta gestión de privilegios	8.0%				0
1.2.1. ¿Se cuentan con políticas donde se regule la disposición de privilegios al sistema?	1.0%			x	1
1.2.2. ¿Se tiene un proceso de autorización debidamente documentado?	1.0%			x	1
1.2.3. ¿Se otorga privilegios de acuerdo a la necesidad basándose las políticas de control de acceso?	1.0%			x	1
1.2.4. ¿Se mantiene un registro de todos los privilegios asignados a los usuarios?	1.0%		x		0.5
1.2.5. ¿Se verifica que no se otorguen privilegios hasta completar el proceso de autorización?	1.0%			x	1
1.2.6. ¿Los privilegios se asignan a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio?	1.0%	x			0
1.2.7. ¿Se revisan las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados?	1.0%			x	1
1.2.8. ¿Se revisan las autorizaciones para los usuarios con privilegios especiales en intervalos de tiempo más cortos?	1.0%			x	1
TOTAL					6.50
1.3. Evaluar los reportes de accesos	4.0%				
1.3.1. ¿Se generan y mantienen registros que provean evidencia de accesos al sistema?	2.0%			x	2
1.3.2. ¿Hay trazabilidad en los registros de acceso al sistema, como: horas de inicio, cierre de sesión y acciones relevantes?	2.0%		x		1
TOTAL					3.00
1.4. Evaluar la realización del procedimiento documentado	4.0%				0
1.4.1. ¿Se cuenta con flujos de trabajos o procedimientos establecidos para el control de accesos?	1.5%			x	1.5
1.4.2. ¿Se realizan las actividades de acuerdo a los procedimientos documentados?	1.0%			x	1
1.4.3. ¿Se realizan auditorias de cumplimiento del control de accesos establecidos en la directiva de seguridad de la información de banco de datos personales?	1.5%			x	1.5
TOTAL					4.00

Figura 37. Resultados post implementación en la Seguridad para el tratamiento de la información Digital (**Fuente**: Elaboración propia)

En la figura 37 se puede observar también que de un total de 30 puntos el área obtuvo un total de 20 puntos.

El indicador 2 “Conservación, respaldo y recuperación de datos personales” fue aplicado en la oficina de Redes y Conectividad, donde se obtuvo el siguiente resultado mostrado en la figura 38.

	VALOR	NO	PARCIAL	SI	TOTAL
2.1 Evaluar el control de seguridad en los ambientes que contienen datos	10.0%				
2.1.1 ¿Los perímetros del edificio o local que contienen los medios de almacenamiento de Información son físicamente solidos?	2.0%			x	2
2.1.2 ¿Las puertas y ventanas están protegidas de accesos no autorizados por mecanismos de control: Por ejemplo vallas, alarmas , relojes, etc.	2.0%			x	2
2.1.3 ¿Los medios de almacenamiento de Información se encuentran físicamente separados de aquellos ajenos a la organización?	2.0%		x		1
2.1.4 ¿Se usan controles de autenticación para restringir el acceso a los ambientes de procesamiento y almacenamiento de Información personal?	2.0%		x		1
2.1.5 EL personal de servicios de ajenos al área ¿cuenta con acceso restringido a las áreas seguras o los medios de procesamiento de Información Personal?	2.0%			x	2
TOTAL					8.00
2.2 Evaluar los Mecanismos de respaldo de la información	8.0%				0
2.2.1 ¿Se mantienen copias de seguridad del banco de datos personales?	1.6%			x	1.6
2.2.2 ¿Las copias de respaldo de datos personales son protegidas mediante técnicas de cifrado?	1.6%	x			0
2.2.3 ¿Las copias de respaldo se almacenan en un lugar físicamente apartado del local principal, para evitar algún daño por algún accidente o desastre natural?	1.6%		x		0.8
2.2.4 La Información de respaldo cuenta con el mismo nivel de seguridad física y ambiental que el local principal.	1.6%		x		0.8
2.2.5 ¿Los medios de respaldos se prueban regularmente para comprobar su correcto funcionamiento?	1.6%			x	1.6
TOTAL					4.80
2.3 Evaluar procedimientos de restauración de respaldos.	7.0%				0
2.3.1 ¿Los procedimientos de restauración se chequean y prueban regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación?	2.0%		x		1
2.3.2 ¿Las pruebas realizadas a los respaldos cuentan con la documentación adecuada?(fecha y hora de la prueba, nombre del que realizo, BDP recuperado, tiempo de recuperación, resultados de la pruebas)	1.0%			x	1
2.3.3 ¿Se toman acciones en caso de pruebas insatisfactorias?	2.0%			x	2
2.3.4 Cuando se restaura una copia de seguridad del banco de datos personales ¿se requiere autorización del titular de BDP o quien es te asignado?	2.0%			x	2
TOTAL					6.00

Figura 38. Resultados post implementación en la Conservación, respaldo y recuperación de datos personales (**Fuente**: Elaboración propia)

Y los indicadores “3. Transferencia lógica o electrónica de datos fue aplicado a la Dirección de DIGETI (ver figura 39) y “4. Prestación de servicios sin acceso a datos personales” respectivamente; el detalle de la evaluación se puede ver en la figura 40.

	VALOR	NO	PARCIAL	SI	TOTAL
3.1. Supervisar la autorización del titular del BDP para la transferencia.	10.0%				
3.1.1. Se cuentan con políticas para la transferencia lógica o electrónica de Datos Personales	2.5%			x	2.5
3.1.2. ¿El tratamiento de datos personales es autorizado por el titular del banco de datos personales?	2.5%			x	2.5
3.1.3. ¿Se cuenta con algún documento que garantice la trasferencia Internacional de Datos Personales?	2.5%			x	2.5
3.1.4. ¿Se procede a la transferencia Datos Personales aun sin la autorización previa del Titular de Banco de Datos o encargado?	2.5%			x	2.5
TOTAL					10.00
3.2. Medios de transporte para la transferencia de datos personales.	10.0%				
3.2.1. ¿Se cuentan con medios de envío autorizados Titular de BDP para la trasferencia de Datos?	2.5%		x		1.25
3.2.2. ¿Se controla el uso de los medios de transferencia de datos personales?	2.5%		x		1.25
3.2.3. ¿Existe evidencia documentada del uso de los medios de transferencia establecidos?	2.5%			x	2.5
3.2.4. ¿Se utilizan software especializado para la transferencia de datos personales?	2.5%	x			0
TOTAL					5.00
3.3. **Mecanismos de Seguridad en la transferencia de Datos Personales**	10.0%				
3.3.1. ¿Se encuentran establecidos los mecanismos de seguridad para la transferencia en las políticas?	2.0%			x	2
3.3.2. ¿Los equipos utilizados para la transferencia lógica cuentan con software de protección contra códigos maliciosos?	2.0%			x	2
3.3.3. ¿Se utilizan protocolos de comunicación cifrados como: VPN, correo electrónico cifrado, FTP seguro, otros?	2.0%			x	2
3.3.4. Los datos contenidos en soporte informático ¿se transportan previa encriptación y un mecanismo de verificación de la integridad?	2.0%	x			0
3.3.5. El Área de tratamiento de datos personales tiene restringido el uso de herramientas de registro no autorizadas? (cámara de video , fotográficas, grabación de audio ,etc.)	2.0%			x	2
TOTAL					8.00

Figura 39. Resultados post implementación en la Transferencia lógica o electrónica de datos (**Fuente**: Elaboración propia)

	VALOR	NO	PARCIAL	SI	TOTAL
TOTAL					8.00
4. Prestación de servicios sin acceso a datos personales	15.0%				
4.1. Servicios internos de la organización o área sin acceso a datos personales	10.0%				
4.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?	2.5%			x	2.5
4.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?	2.5%			x	2.5
4.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.	2.5%			x	2.5
4.1.4. ¿Se generan documentos mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?	2.5%	x			0
TOTAL					**7.5**
4.2. Servicios externos a la organización sin acceso a datos personales	5.0%				
4.2.1. ¿Se generan contratos expresos o cláusulas contractuales sobre el tratamiento de datos personales al momento de prestar servicios externos?	1.25%			x	1.25
4.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?	1.25%			x	1.25
4.2.3. ¿Existe algún documento que garantice la destrucción o imposibilidad de recuperación de los datos alojados en el servicio del prestador de servicio una vez concluida la relación con el proveedor?	1.25%		x		0.625
4.2.4. ¿Se realizan visitas a la infraestructura del proveedor para comprobar el cumplimiento del servicio? O en caso de un proveedor extranjero: ¿Los prestadores de servicio cuentan con reportes SOC para verificar el cumplimiento del servicio?	1.25%		x		0.625
TOTAL					**3.8**

Figura 40. Resultados post implementación en la Prestación de servicios sin acceso a datos personales (**Fuente**: Elaboración propia)

Por otro lado, la evaluación final para Secretaria General fue realizada en la primera semana del mes de febrero del 2018, y se realizó con las encargadas del área de

Archivo Académico Institucional, Registro Académico, y Registro Administrativo en conjunto, y se obtuvieron los siguientes resultados:

Almacenamiento, copia y acceso la documentación no automatizada.

Como se puede ver en la figura 43 el puntaje obtenido por cada rubro dentro del factor primario de Almacenamiento copia y acceso es aprox. 48 de 50 puntos.

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
1. Almacenamiento, copia y acceso a la documentación no automatizada	**50.0%**				
1.1. Almacenamiento de documentación no automatizada	**20.0%**				
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.	8.0%			x	8
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?	6.0%			x	6
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?	6.0%			x	6
TOTAL	**20.0%**				**20**
1.2. Copia o reproducción de la documentación no automatizada	**15.0%**				
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?	3.0%			x	3
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales sin permitir su recuperación.	3.0%			x	3
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?	3.0%			x	3
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos	3.0%			x	3
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?	3.0%			x	3
TOTAL	**15.0%**				**15**
1.3. Acceso a la documentación no automatizada	**15%**				
1.3.1 ¿Se cuenta con algún documento donde indique la responsabilidad que recae en el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos personales?	3.75%			x	3.75
1.3.2 ¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?	3.75%			x	3.75
1.3.3 ¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?	3.75%		x		1.875
1.3.4 ¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?	3.75%			x	3.75
TOTAL	**15.0%**				**13.125**

Figura 41. Resultados post implementación en el Almacenamiento, copia y acceso a la documentación no automatizada (**Fuente**: Elaboración propia)

Traslado de documentación no automatizada

En el traslado de documentación se obtuvo un total de 22 de 30 puntos en la evaluación, como se puede observar en la figura 42.

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
2. Traslado de la documentación no automatizada	**30%**				
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado	**17.5%**				
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?	2.5%			x	2.5
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?	2.5%			x	2.5
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?	2.5%		x		1.25
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?	2.5%			x	2.5
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?	2.5%		x		1.25
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?	2.5%	x			0
2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.	2.5%	x			0
TOTAL	**17.5%**				**10**
2.2. Eventos o incidentes en el traslado de datos personales	**12.5%**				
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?	4.5%			x	4.5
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?	4.0%			x	4
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?	4.0%			x	4
TOTAL					**12.5**

Figura 42. Resultados post implementación en el Traslado de documentación no automatizada (**Fuente**: Elaboración propia)

5.5. Etapa 5: Determinación del nivel de mejora

La etapa 5 comprende 2 actividades que fueron realizadas teniendo como insumos los resultados de la evaluación post implementación:

En primer lugar, se hizo el análisis de los resultados de los check list obtenidos en la evaluación, para esto se elaboró un cuadro consolidado de los resultados tanto del área de Secretaria General, así como de DIGETI.

Finalmente se logró determinar los siguientes puntos:

- En cuanto a Seguridad para el tratamiento de la información Digital se alcanzó un porcentaje del **85%** de cumplimiento gracias a la implementación del proceso de gestión de usuarios y el establecer un documento formal de políticas para el área.

- En la conservación, respaldo y recuperación de los datos personales el porcentaje alcanzado es de **75.5 %** de cumplimiento en ese factor, la implementación de políticas, los documentos, formatos, procedimientos para el respaldo y restauración fueron claves para alcanzar el nivel.

- En cuanto a la Transferencia lógica o electrónica, a pesar de que se hizo propuestas sobre políticas para la transferencia de datos a entidades internas y externas, formatos que evidencien el proceso de autorización de transferencias, y debido a que se necesitaba de una inversión de recursos considerables no se logró aplicar algunas recomendaciones que se dieron en las propuestas en cuanto al uso de software especializado para el encriptamiento de datos a la hora de realizarse una transferencia. Por lo cual el resultado es un **76.6 %** alcanzado.

- Sobre la Prestación de Servicios sin acceso a datos personales, en el caso de DIGETI el establecimiento de políticas internas evidenció que se hace un mejor control cuando una persona ajena al área realiza algún servicio en sus oficinas. En los contratos con servicios externos que DIGETI puede realizar también se establecieron las cláusulas de confidencialidad, lo que se evidenció en el resultado de **75%** los estándares cumplidos alcanzados. En el caso de Secretaria General se aplicaron unas recomendaciones y el compromiso de confidencialidad ya que como se indicó en la Etapa 3 ellos no realizan contratos propios por lo que este indicador no aplica al área.

- En los indicadores de Almacenamiento, copia y acceso a la documentación se implementaron de manera exitosa los formatos para evidenciar el acceso al área del Banco de Datos, el envío de archivos fuera de área y fuera de la institución, el proceso de destrucción de documentos mediante la adquisición de una máquina trituradora, el procedimiento de gestión de incidentes, cuyo indicador a la fecha es de cero incidentes reportados evidencian el resultado de 96.6 **%** alcanzado.

- En el traslado de la documentación no automatizada también se evidenció un **75 %** alcanzado ya que se mejoró el procedimiento de traslado de documentos con la implementación de formatos y políticas con las que antes no contaban.

CAPÍTULO VI: RESULTADOS DE LA INVESTIGACIÓN

6.1. Análisis de los resultados

Para hacer un análisis de los resultados obtenidos y conocer sobre el nivel de mejora en comparación a la evaluación pre implementación se realizaron las siguientes tablas.

Tabla 17
Tabla de resultados de evaluación post implementación en DIGETI

Factores primarios	Peso x factor	Puntaje alcanzado	Porcentaje alcanzado	Resultado Cualitativo
1.Seguridad para el tratamiento de la Información Digital	30 %	25.5	85 %	ALTO
2.Conservación, respaldo y recuperación de Datos Personales	25 %	18.8	75.2 %	ALTO
3. Transferencia lógica o electrónica de Datos Personales.	30 %	23	76.6%	ALTO
4.Prestación de servicios sin acceso a datos personales	15 %	11.25	75%	ALTO
Total	100%	78.55		ALTO

En la tabla 17 se muestra que en DIGETI se obtuvo un nivel ALTO en el cumplimiento en cada factor primario de los artículos de la ley que tratan sobre medidas de Seguridad para un Banco de Datos Automatizado.

De la misma manera en la tabla 18 se evidencia que se alcanzó un nivel ALTO en cuanto el uso de controles de seguridad para un Banco de Datos no Automatizado.

Tabla 18
Tabla de resultados de evaluación post implementación en Secretaría General

Factores primarios	Peso x factor	Puntaje alcanzado	Porcentaje alcanzado	
1. Almacenamiento, copia y acceso a la documentación no automatizada	50 %	48.125	96.25 %	ALTO
2. Traslado de la documentación no automatizada	30 %	22.5	75 %	ALTO
3. Prestación de servicios sin acceso a datos personales.	20 %	9.75	48.75%	MEDIO
Total	100%	80.375		ALTO

Finalmente, en la Tabla 19 se presenta una comparación de los porcentajes alcanzados pre y post implementación mostrando una mejora en cuanto al nivel de un 24 % por medio de la implantación de controles.

Tabla 19
Comparación entre las evaluaciones pre implementación y post evaluación de DIGETI y Secretaría General

Factores Primarios	% Total	% Alcanzado Pre	% Alcanzado Post
Dirección General de Tecnologías de Información			
1.Seguridad para el tratamiento de la Información Digital	30	14	25.5
2.Conservación, respaldo y recuperación de Datos Personales	25	18.8	18.8
3. Transferencia lógica o electrónica de Datos Personales.	30	15.75	23
4.Prestación de servicios sin acceso a datos personales	15	5.63	11.25
Total	100	54.2	78.55
Secretaría General			
1. Almacenamiento, copia y acceso a la documentación no automatizada	50	29.38	48.125
2. Traslado de la documentación no automatizada	30	12	22.5
3. Prestación de servicios sin acceso a datos personales.	20	2.5	9.75
Total	100	43.88	80.375

En Secretaría General de la misma manera se muestra una mejora de aproximadamente 40 % y resaltando más en el primer factor donde era el más crítico en la evaluación previa.

La figura 43 muestra de manera gráfica las mejoras alcanzadas por cada factor primario o artículo de la Ley.

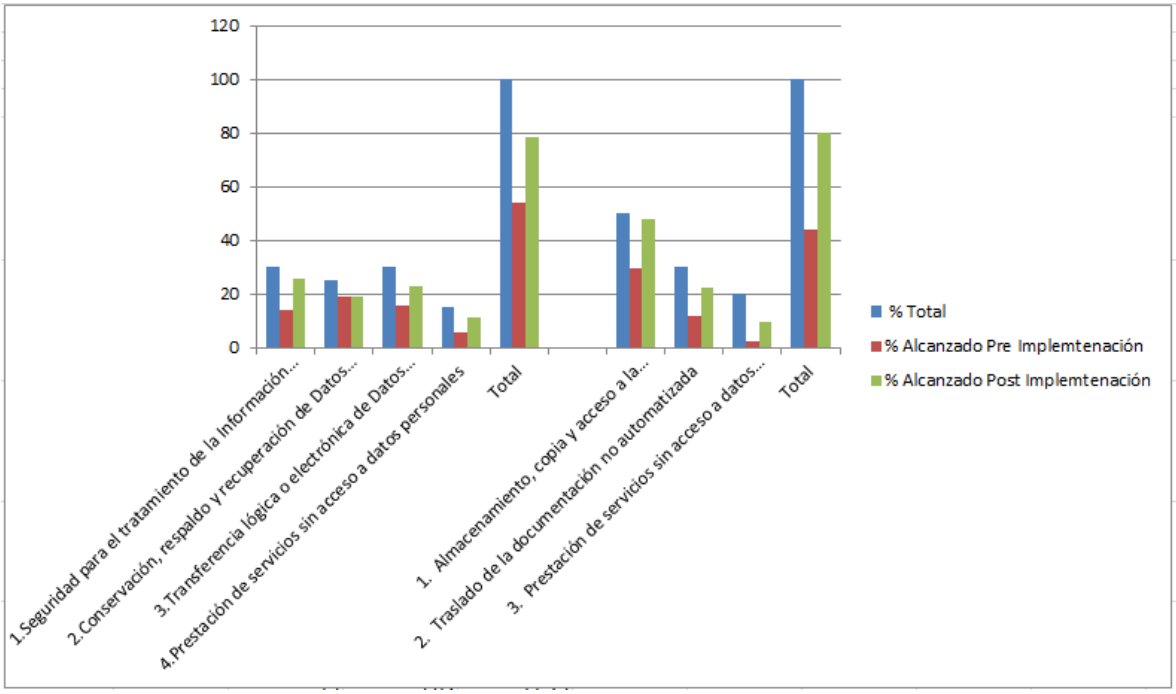


Figura 43. Gráfico de barras del porcentaje total, pre implementación y post implementación (**Fuente**: Elaboración propia)

CAPÍTULO VII: CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

- Se realizó una evaluación preliminar de cumplimiento del Reglamento de la LPDP a las áreas comprometidas. En DIGETI se evidenció un 54,2 % de cumplimiento (ver Tabla 7), y en Secretaría General un 43,8% (ver Tabla 8).
- Se desarrolló un plan de mejora basado en los controles de seguridad de acuerdo a la NTP-ISO/IEC 17799:2007. La propuesta de controles para DIGETI se puede apreciar en anexo 9, y la propuesta de controles para Secretaría General en el anexo 10.
- Se implementó controles de seguridad para el cumplimiento del Capítulo V "Medidas de Seguridad" del Reglamento de la LPDP, la aprobación del jefe de DIGETI se demuestra en la figura 34 y la de Secretaría General en la figura 35. Así mismo se programó reuniones de concientización al personal de las áreas afectadas, tal y como lo muestra el anexo 7 para DIGETI y 13 para Secretaría General.
- Se realizó una evaluación al área comprometida para identificar el nivel de cumplimiento post implementación. En DIGETI se demostró 78,55% de cumplimiento (ver tabla 17), y en Secretaría General un 80,37 (ver tabla 18).
- Se evidenció mediante entregables el nivel de mejora alcanzado en las medidas de seguridad para la protección de datos personales. Los controles implementados se manifiestan en los anexos, y el cuadro de comparación entre las evaluaciones pre y post implementación se aprecia en la tabla 19.

Finalmente, se concluye que se implementó controles de seguridad basados en la NTP-ISO/IEC 17799:2007 para el cumplimiento parcial de la Ley de Protección de Datos Personales nro. 29733 en una Universidad Privada.

7.2. Recomendaciones

- Se recomienda hacer un diagnóstico de áreas críticas (DAC) para identificar las áreas de aplicación en otras empresas o instituciones en las cuales se desee aplicar o ejecutar este proyecto.
- Se recomienda a la dirección de DIGETI y Secretaría General impulsar el cumplimiento de los controles aprobados en sus respectivas áreas, logrando así; cumplir con la normatividad peruana y adoptar una cultura de seguridad de la información en la organización.
- Se recomienda implementar las propuestas que incluyen inversiones económicas para mejorar los equipos o herramientas que aseguren la confidencialidad y seguridad de la información.
- Se recomienda realizar una revisión periódica de cumplimiento de controles y demás requisitos y cambios de la Ley de Protección de Datos Personales y su Reglamento.
- Se recomienda importante que tomen esta tesis como base para la implementación de futuros controles.
- Se recomienda con carácter de urgencia desarrollar un plan de cumplimiento para la Ley de Protección de Datos Personales a nivel corporativo, que el desarrollo de este plan pueda ser elaborado en conjunto por el área legal, administrativo y tecnológico; además, que su alcance comprenda todo el personal, sus procesos y tecnologías de la organización.
- Se recomienda importante implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la UPeU, y que este SGSI contemple el cumplimiento normativo de la Ley de Protección de Datos Personales.

BIBLIOGRAFÍA

Abdellah FG, Levine (1994) E. Preparing Nursing Research for the 21 st Century. Evolution. Methodologies, Chalges. Springer: New York.

Autoridad Nacional de Protección de Datos Personales. (2013). Reglamento Ley de Protección de Datos Nro 29733. *El Peruano*, (35), 27-45.

Congreso Constituyente del, P. (1993). Constitución política del Perú, 1-60.

Congreso de la República del Perú. (2011). Ley de protección de datos personales LEY Nº 29733. *Sistema Peruano de INformación Jurídica*, 1-17. Recuperado a partir de http://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

Council of Europe. (1985). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Recuperado 15 de febrero de 2018, a partir de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Cruzatt, K. C. (2005). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú, (1), 260-276.

Deloitte. (2015). Ley de Protección de Datos Personales. Enfoque práctico de adecuación., 41. Recuperado a partir de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Privacidad/Ley de Protección de Datos Personales de COL - Enfoque Práctico vdef.pdf

Edición, P., de Justicia Derechos Humanos, M., Figallo Rivadeneyra Viceministro de Derechos Humanos Acceso la Justicia, D., José Ávila Herrera, H., & Álvaro Quiroga León Edición, J. (s. f.). Directiva De SeguriDaD autoridad Nacional de Protección de Datos Personales aPDP Director de la Autoridad Nacional de Protección de Datos Personales. Recuperado a partir de www.minjus.gob.pe

Empresariales, F. D. E. C. (2017). Universidad peruana unión.

ESAN. (2016). Norma Técnica Peruana: políticas y procedimientos en seguridad de información | | Apuntes empresariales | ESAN. Recuperado 13 de febrero de 2018, a partir de https://www.esan.edu.pe/apuntes-empresariales/2016/04/norma-tecnica-peruana-politicas-procedimientos-seguridad-informacion/

Forum, W. E. (2017). | Global Risks Report 2017 - Reports - World Economic Forum. Recuperado 11 de febrero de 2018, a partir de http://reports.weforum.org/global-risks-2017/global-risks-landscape-2017/?doing_wp_cron=1518380896.8941509723663330078125#landscape///technological

GTDI. (2015). Alcances sobre la Directiva de Seguridad para la ley de protección de datos personales | Tecnologías de la Información y Consultoria. Recuperado 13 de febrero de 2018, a partir de http://www.gtdi.pe/alcances_sobre_directiva_de_seguridad

Herrero, P. (2012). La importancia de la visión «end to end» en la empresa - Blog Sage Experience. Recuperado 13 de febrero de 2018, a partir de https://blog.sage.es/economia-empresa/la-importancia-de-la-vision-«end-to-end»-en-la-empresa/

ISO/IEC. (2007). NTP-ISO / IEC 17799 EDI. Tecnología de la información . Código de buenas. *El Peruano*, *2a. Edició*(Lima 41), 179. Recuperado a partir de http://www.iso.org/iso/catalogue_detail?csnumber=39612

Jimeno Bernal, J. (2013). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua | PDCA Home. Recuperado 11 de febrero de 2018, a partir de https://www.pdcahome.com/5202/ciclo-pdca/

López Torres, J. (2010). ANTECEDENTES INTERNACIONALES EN MATERIA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES, *1*(19), 1-19.

Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de

datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)*, *30*(1), 77-96. https://doi.org/10.4067/S0718-09502017000100004

MINJUS, A. de E. (2018). Asistente de Evaluación sobre Requisitos de Seguridad Implementados Tipo de tratamiento : Complejo, 13-14.

ONU. (1948). Declaración Universal De Derechos Humanos, (3), 1-5. https://doi.org/10.1017/CBO9781107415324.004

Plaza, É. (s. f.). La importancia del Compliance y la Prevención de Riesgos Corporativa | El Jurista. Recuperado 13 de febrero de 2018, a partir de http://www.eljurista.eu/2015/01/04/la-importancia-del-compliance-y-la-prevencion-de-riesgos-corporativa/

Sánchez Pérez, G., & Rojas González, I. (s. f.). LEYES DE PROTECCIÓN DE DATOS PERSONALES EN EL MUNDO Y LA PROTECCIÓN DE DATOS BIOMÉTRICOS. *https://revista.seguridad.unam.mx*. Recuperado a partir de https://revista.seguridad.unam.mx/printpdf/2124

Unión, U. P. (s. f.). Misión y Visión - UPeU. Recuperado 7 de febrero de 2018, a partir de http://www.upeu.edu.pe/mision-y-vision/

ANEXOS

Anexo 1. Plan de auditoría de DIGETI y Secretaría General

UNIVERSIDAD
PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

PLAN DE AUDITORÍA

EVALUACIÓN A LAS MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN AUTOMATIZADA PARA EL CUMPLIMIENTO DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

Lizeth Reaucan 10-10-16.

Elicer Carlos 10/10/16

Reunión: Miércoles 12/10/16 11:00 am

Equipo auditor	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Lima, Octubre 2016

UNIVERSIDAD
PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

PLAN DE AUDITORÍA

EVALUACIÓN A LAS MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN AUTOMATIZADA Y NO AUTOMATIZADA PARA EL CUMPLIMIENTO DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

Secretaría General

Reunión con el personal 13 y 14 de octubre.

Equipo auditor	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Lima, Octubre 2016

RESUMEN EJECUTIVO

En la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones que tienen como objetivos apoyar en cuanto a la toma de decisiones y en la gestión de una organización. Estos sistemas están en constante actualización ya que se adecuan a las necesidades emergentes, lo que hace a la vez que se rijan estándares para asegurar las buenas prácticas en la creación e implementación, y el uso de los mismos. En este caso el Estado Peruano ve por conveniente la creación de una normativa que asegure un buen uso de la Información que contienen estos sistemas.

La Ley Nro. 29733 "Ley de Protección de Datos Personales del Perú" tiene como objetivo proteger los datos personales de personas naturales que estén bajo la gestión de empresas públicas y privadas.
En el Artículo 16 de la mencionada Ley, "Seguridad para el tratamiento de datos personales" expresa que para fines del tratamiento de datos personales se debe garantizar la seguridad a través de medidas técnicas, organizativas y legales, evitando su alteración, pérdida o acceso no autorizado. Los requisitos y condiciones de seguridad son establecidos por la Autoridad de Protección de Datos Personales (ANDPD) a través del Título V de su reglamento.

Actualmente, DIGETI (Dirección General de Tecnologías de Información) cuenta con medidas de seguridad básicas que han sido implementadas de acuerdo a la necesidad, como por ejemplo la protección de BackUps por medio del software "R1Soft" y la gestión de accesos a información por medio del Sistema Académico.

Secretaria General es un área dentro de la Universidad en la cual se realizan la mayoría de tramites documentarios, así como el almacenamiento de información personal, de alumnos por lo cual, es necesario que se implementen medidas de seguridad acorde a la necesidad y a la vez a la ley, para no sufrir perdida de información o caer en infracciones legales.

La finalidad de la presente Auditoría es evaluar el nivel de cumplimiento que tiene el área de DIGETI y Secretaría General en el tratamiento de datos personales automatizados y no automatizados respectivamente, con respecto a la Ley N° 29733 (LPDP) y apoyándonos en la NTP-ISO/IEC 17799:2007, proponiendo posteriormente mejoras en función a los resultados.

DESCRIPCIÓN DE LA ORGANIZACIÓN

1. Datos generales de la organización

1.1. Razón social: Universidad Peruana Unión

1.2. Rubro o giro del negocio: Educación

1.3. Dirección: Km 19 Carretera Central, Ñaña (Prolong. Bernardo Balaguer)

1.4. Representante legal: Sara Flor Ticona Mamani

2. Descripción de las principales actividades de la organización

2.1 Educación:

- La UPeU ofrece educación básica y en la superior las modalidades de presencial y a distancia. La Universidad cuenta también con dos filiales (Juliaca y Tarapoto), locales universitarios y centros de aplicación.
  Los datos personales registrados, almacenados y/o utilizados de acuerdo a la finalidad de recopilación de cada área, son alojados en servidores internos (Perú, UPeU) y externos (USA, Amazon) dependiendo del área.

2.2 Venta de productos alimenticios:

- La organización cuenta también con el área de "Productos Unión" que en conjunto con la Universidad promueve una alimentación saludable.

2

Esta área es encargada también de administrar los datos personales de sus clientes y proveedores alojados en los servidores de DIGETI.

2.3 Generar oportunidad laboral:

- La universidad ofrece también oportunidad laboral para los estudiantes y egresados dentro de las distintas áreas de la Universidad.
  Esta actividad es llevada a cabo por el área de RR.HH, encargados también de tratar los datos personales de los colaboradores de toda la empresa con la colaboración de DIGETI.

2.4 Visión

"Ser una Universidad modelo, acreditada, reconocida en la Iglesia Adventista del Séptimo Día y la sociedad por la práctica de valores cristianos y su espíritu misionero."

2.5 Misión:

"La Universidad Peruana Unión es una institución educativa de la Iglesia Adventista del Séptimo Día que forma integralmente profesionales e investigadores competentes y creativos, capaces de brindar un servicio cristiano a la Iglesia y sociedad para restaurar en el ser humano la imagen de Dios."

3. Objetivos de la auditoría de sistemas

3.1. Objetivo general

- Evaluar el cumplimiento de la Ley N° 29733 "Ley de Protección de Datos Personales" en los procesos del área de DIGETI y Secretaria General de la UPeU.

3.2. Objetivos específicos

- Realizar una evaluación a la seguridad física y del entorno a los equipos de TI (Tecnología de la Información) para salvaguardar los datos personales.
- Realizar una evaluación a la gestión de las comunicaciones y operaciones en las áreas de aplicación especificadas.
- Evaluar el control de accesos de los usuarios que tienen acercamiento a los datos personales.
- Realizar una evaluación del almacenamiento, copia, y acceso de información no automatizada.
- Evaluar el control en el traslado de la información no automatizada.
- Realizar una evaluación de la prestación de servicios sin acceso a los datos personales.

4. Descripción de la situación actual del área a evaluar

4.1. Nombre del área

Áreas: DIGETI (Dirección General de Tecnologías de Información) y Secretaría General.

4.2. Descripción de las principales actividades del Área

✓ **Área de DIGETI**

a) Área de redes y conectividad
- Esta área está encargada de dar soporte a las redes informáticas y administrar los servidores físicos y virtuales de la UPeU.

b) Área de desarrollo de software
- Esta área es la encargada de dar soporte y mantenimiento a los Sistemas de Información de la UPeU, como también tener accesos especiales al sistema y a los datos personales.

c) Área de Dirección general
- Dentro de esta área se encuentran las personas que gestionan los pedidos, costos y los negocios con los proveedores, por lo que es de total importancia su participación en el área por el conocimiento amplio y experiencia que tienen.

d) Área de mesa de ayuda
- Esta área se encarga de brindar servicios de apoyo técnico a alumnos y trabajadores de la universidad, como también la creación y administración de los usuarios y correos institucionales.

e) Área de coordinación de servicios computacionales
- Verificar la operatividad del equipo en la sala que se administra.
- Efectuar el mantenimiento preventivo y correctivo al hardware y software para garantizar una máxima disponibilidad de servicio.
- Dar servicio informático al docente y al alumno.

✓ **Área de Secretaría General**

a) Trámite documentario
b) Grados y Títulos
c) Estadística e Información
d) Archivo institucional
e) Registro y actas académicos
f) Registro y actas administrativos

4.3. Relación de puestos y principales funciones

1. **Área de DIGETI**

Nombre del puesto	Funciones
Director General de DIGETI	Liderar el área de DIGETI, y realizar las distintas negociaciones con proveedores para beneficio de la universidad.
Supervisor de Redes y Comunicaciones	Encargado de supervisar y velar por el buen funcionamiento y mantenimiento de las redes y equipos que almacenan información
Supervisor de Soporte y mesa de ayuda	Encargado de brindar servicio técnico para los equipos (Hardware y Software) dentro de la universidad.
Mantenimiento y soporte en el Área de Desarrollo de Software	Encargado de dar soporte y mantenimiento a los sistemas de información dentro de la Universidad Peruana Unión.

2. **Área de Secretaría General**

Nombre del puesto	Funciones
Secretario General	Dar fe con su firma a los acuerdos y documentos oficiales que elaboran y emiten las autoridades de la UPeU, dirige el sistema de Tramites Documentarios, organiza y dirige el Archivo Central Académico y Administrativo.

4.4. Descripción de las tecnologías de información

1. **Área de DIGETI**

Nombre de la TI	Descripción
Hardware	
Servidores: Dell y HP	Almacenamiento de información y/o brindar servicios.
Computadoras de escritorio y Laptops	Para el uso en las actividades correspondientes, acceso al sistema, etc.
Storage	Red de almacenamiento integral
Sistema Operativo	
Linux (Centos y Ubuntu) Windows 2008r2 y Estándar Windows 2012	S.O dependiendo de la finalidad del servidor.

5

Windows 7, 8 y 10	S.O para las Pc´s de las oficinas.
Software	
R1SOFT (Server Backup Manager)	Software para la realización de Backups en los servidores.
VMware ESXI 5.5	Software para administrar particiones múltiples (Máquinas Virtuales)
MySQL SGBD ORACLE SQL Server	Gestor de base de datos para dar soporte, estabilidad y administración de los datos.
Servicios	
Active Directory (AD)	Administrar grupos, usuarios y privilegios de usuario dentro de la red.

2. **Área de Secretaría General**

Nombre de la TI	Descripción
Hardware	
Pc's de Escritorio.	Para la redacción de los documentos, el envío de información y otras tareas propias de cada puesto.
Impresoras.	Dispositivos utilizados para la impresión de los documentos, estos se encuentran compartidos dentro de un área para el trabajo conjunto.
Sistema Operativo	
Windows 7	S.O. para las Pc's de las oficinas.
Windows 8	S.O. para las Pc's de las oficinas administrativas.
Software	
Microsoft Office 2013	Software para realizar documentos, hojas de cálculos, presentaciones, etc.

6

5. Aspectos de evaluación que contempla la auditoría de sistemas

La Ley Nro. 29733 en su Artículo 16 declara que:

5.1. Artículo 16 (LPDP). Seguridad del tratamiento de datos personales:

Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.

a) Aspectos de Evaluación para DIGETI

El reglamento de la Ley Nro. 29733 en sus Artículos 39, 40 y 41 declaran que:

i. Artículo 39 (Reglamento). Seguridad del tratamiento de información digital.

Los Sistemas de Información deberán incluir:

1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.
2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.
   Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.

ii. Artículo 40 (Reglamento). Conservación, respaldo y recuperación de los datos personales.

Los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la "NTP ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información." en la edición que se encuentre vigente. Adicionalmente, se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el

respaldo, incluyendo cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.

iii. **Artículo 41 (Reglamento). Transferencia lógica o electrónica de los datos personales.**
El intercambio de datos personales desde los ambientes de procesamiento o almacenamiento hacia cualquier destino fuera de las instalaciones físicas de la entidad, sólo procederá con la autorización del titular del banco de datos personales y se hará utilizando los medios de transporte autorizados por el mismo, tomando las medidas necesarias, entre las que se encuentran cifrado de datos, firmas digitales, información, checksum de verifi cación, entre otros, destinados a evitar el acceso no autorizado, pérdida o corrupción durante el tránsito hacia su destino.

b) Aspectos de Evaluación para Secretaría General
El reglamento de la Ley Nro. 29733 en sus Artículos 42, 43, 44, 45, 46 declaran que:

i. **Artículo 42 (Reglamento). Almacenamiento de documentación no automatizada.**
"... Los armarios archivadores y otros elementos en los que se almacenan documentos no automatizados con datos personales deberán encontrarse en áreas en las que el acceso este protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el banco de datos.
Si por las características de los locales que se dispusiera no fuera posible cumplir lo establecido en el apartado anterior, se adoptarán las medidas alternativas, conforme a las directivas de la Dirección General de Protección de Datos Personales..."

ii. **Artículo 43 (Reglamento). Copia o reproducción.**
"La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior."

iii. **Artículo 44 (Reglamento). Acceso a la documentación.**
"El acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo a las directivas de seguridad que emita la Dirección General de Protección de Datos Personales."

iv. **Artículo 45 (Reglamento). Traslado de documentación no automatizada.**

8

"Siempre que se proceda al traslado físico de la documentación contenida en un banco de datos, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado."

v. **Artículo 46 (Reglamento). Prestaciones de servicios sin acceso a datos personales.**
"El responsable o el encargado de la información o tratamiento adoptarán las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio."

c) Controles de la NTP-ISO/IEC 17799:2007
La Norma Técnica es un documento que contiene buenas prácticas de gestión de la seguridad de la información. Su propósito es presentar una serie de recomendaciones para realizar una correcta gestión de seguridad de la información y servir de guía para adoptar o implementar estándares de seguridad en las organizaciones.

Para la evaluación del presente plan de auditoría se utilizaron las siguientes clausulas:

1. **Seguridad física y del entorno.**
2. **Gestión de comunicaciones y operaciones.**
3. **Control de Acceso.**
4. **Gestión de incidentes de los sistemas de información.**
5. **Cumplimiento.**

6. Alcance

El alcance de la auditoría es la evaluación del cumplimiento de los Artículos 39, 40, 41, 42, 43, 44, 45, 46 del Reglamento de la Ley Nro. 29733, tomando como referencia para el cumplimiento los controles 9, 10, 11, 13 y 15 de la NTP-ISO/IEC 17799:2007.

7. Limitaciones

a) El reglamento de la Ley de Protección de Datos Personales contiene 4 principios rectores, los siguientes principios no abarcara el proyecto:

1. **Principios rectores:**
   i. Artículo 6.- Principio de consentimiento
   ii. Artículo 7.- Principio de finalidad
   iii. Artículo 8.- Principio de calidad

b) La NTP-ISO/IEC 17799:2007 contiene 11 cláusulas control, las siguientes no abarcaran el proyecto:

2. Cláusulas de control de seguridad

i. Aspectos Organizativos para la seguridad
ii. Clasificación y control de activos
iii. Seguridad en recursos humanos
iv. Adquisición y mantenimiento de sistemas
v. Gestión de la continuidad del negocio

8. Guía de ponderación para la evaluación de medidas de seguridad de la información automatizada y no automatizada.

8.1. Factores primarios para la información automatizada (DIGETI)

Factores primarios	Peso por factor	Valor % Específico
Evaluación de Medidas de Seguridad de los datos personales automatizados		**100%**
1. Seguridad para el tratamiento de la Información Digital	**35%**	
2. Conservación, respaldo y recuperación de los datos personales.	**30%**	
3. Transferencia Lógica o Electrónica de los Datos Personales	**35%**	
	100%	-

Tabla 1. Factores primarios de la evaluación para la información automatizada

- **Evaluación N° 1**

Actividades a ser evaluadas y ponderadas	Peso por actividad	Peso por factor a ponderar	Valor de ponderación
1. Seguridad para el tratamiento de la Información Digital			**35%**
1.1 Control de acceso a la información(DP)	**35%**	**12,25%**	
1.2 Gestión de privilegios	**20%**	**7,00%**	
1.3 Reportes de Accesos	**25%**	**8,75%**	
1.4 Documentación del Procedimiento	**20%**	**7,00%**	
	100%	**35,00%**	

Tabla 2. Actividades a evaluar y ponderar la seguridad para el tratamiento de la información digital

- **Evaluación N° 2**

Actividades a ser evaluadas y ponderadas	Peso por actividad	Peso por factor a ponderar	Valor de ponderación
2. Conservación, respaldo y recuperación de los datos personales.			30%
2.1 Control de Seguridad en ambiente de datos	40%	12,00%	
2.2 Mecanismos de Respaldo para la Seguridad de la Información (BDP)	60%	18,00%	
	100%	30,00%	

Tabla 3. Actividades a evaluar y ponderar de la conservación, respaldo y recuperación de los datos personales

- **Evaluación N° 3**

Actividades a ser evaluadas y ponderadas	Peso por actividad	Peso por factor a ponderar	Valor de ponderación
3. Transferencia lógica o electrónica de Datos Personales			**35%**
3.1 Autorización del Titular del BDP para la transferencia	**40%**	**14,00%**	
3.3 Medio de transporte autorizado por el titular de BDP	**30%**	**10,50%**	
3.2 Mecanismos de cifrado de Datos para la transferencia	**30%**	**10,50%**	
	100%	**35,00%**	

Tabla 4. Actividades a evaluar y ponderar la transferencia lógica o electrónica de datos personales

8.2. Factores primarios para la información no automatizada (Secretaría General)

Factores primarios	Peso por factor	Valor % Específico
Evaluación de Medidas de Seguridad de los datos personales no automatizados		**100 %**
1. Almacenamiento, copia, y acceso de información no automatizada.	**50 %**	
2. Traslado de la información no automatizada.	**30 %**	
3. Prestación de servicios sin acceso a datos personales.	**20 %**	
	100 %	

Tabla 5. Factores primarios de la evaluación para la información no automatizada

11

- **Evaluación N° 1**

Actividades a ser evaluadas y ponderadas	Peso por actividad	Peso por factor a ponderar	Valor de ponderación
1. Almacenamiento, copia, y acceso a la información no automatizada.			50%
1.1 Almacenamiento de documentación no automatizada	35%	20%	
1.2 Copia o reproducción de la documentación no automatizada	30%	10%	
1.3 Acceso a la documentación no automatizada	35%	20%	
	100%	50,00%	

Tabla 6. Actividades a evaluar y ponderar el almacenamiento, copia y acceso de la información no automatizada

- **Evaluación N° 2**

Actividades a ser evaluadas y ponderadas	Peso por actividad	Peso por factor a ponderar	Valor de ponderación
2. Traslado de la documentación no automatizada			30%
2.1 Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado	55%	20%	
2.2 Eventos o incidentes en el traslado de datos personales	45%	10%	
	100%	30,00%	

Tabla 7. Actividades a evaluar y ponderar el traslado de la documentación no automatizada

- **Evaluación N° 3**

Actividades a ser evaluadas y ponderadas	Peso por actividad	Peso por factor a ponderar	Valor de ponderación
3. Prestación de servicios sin acceso a datos personales			20%
3.1 Servicios internos de la organización o área sin acceso a datos personales	48%	9%	
3.2 Servicios externos a la organización sin acceso a datos personales	52%	11%	
	100%	20,00%	

Tabla 6. Actividades a evaluar y ponderar la prestación de servicios sin acceso a datos personales

12

9. Cronograma de la auditoría

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
	Actividades para la realizacion de la auditoria	13 días	sáb 01/10/16	mar 18/10/16
	Planificacion de la Auditoria	8 días	sáb 01/10	mar 11/1
	Levantamiento de la informacion DIGETI	3 días	sáb 01/10/16	mar 04/10/16
	Levantamiento de Informacion Secretaria General	3 días	mié 05/10/16	vie 07/10/16
	Formulacion del plan de auditoria	5 días	lun 03/10	vie 07/10
	Validacion del plan de auditoria e instrumentos	3 días	dom 09/10/16	mar 11/10/16
	Ejecucion de la Auditoria.	6 días	dom 09/1	vie 14/10
	Presentacion del plan a las áreas a auditar	2 días	lun 10/10/16	mar 11/10/16
	Visita al Área para aplicar el instrumento (DIGETI)	2 días	mié 12/10/16	jue 13/10/16
	Visita al area para aplicar el instrumento (Secretaria General)	2 días	jue 13/10/16	vie 14/10/16
	Dictamen de la Auditoria	3 días	jue 13/10	lun 17/10
	Realizacion del Dictamen Final de auditoria	2 días	vie 14/10/16	sáb 15/10/16
	Presentacion del dictamen final de Auditoria	1 día	lun 17/10/16	lun 17/10/16

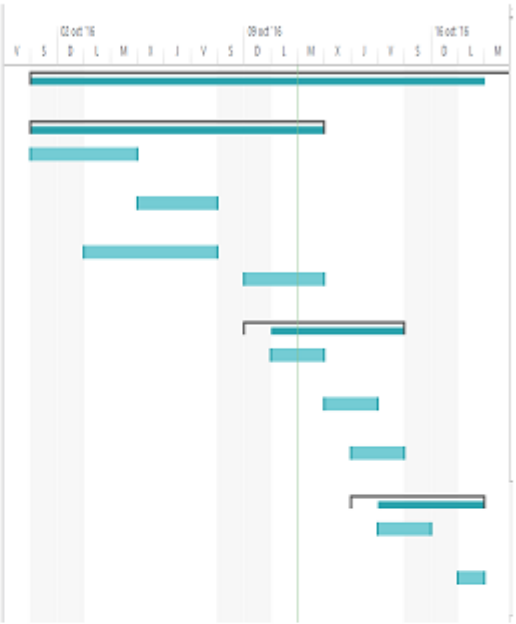


Tabla 7. Actividades de la auditoría

13

10. Guía de auditoría para evaluar el nivel de cumplimiento de la Ley N° 29733 en la Universidad Peruana Unión.

10.1. Guía de la auditoría para la evaluación de la información automatizada (DIGETI)

- Guía de auditoría para la evaluación del tratamiento de la información digital

Guía de auditoría para la evaluación del cumplimiento de Seguridad para el tratamiento de la Información Digital					
Propietario del documento: Equipo Auditor		Universidad Peruana Unión Área: Dirección General de Tecnologías de Información		Fecha:	Hoja 1 de 3
Ref.	Actividad que será evaluada	Procedimientos de auditoría	Herramientas que serán utilizadas	Recursos	Observaciones
DG001	Evaluar el Control de acceso a la información(DF)	1. Solicitar el permiso para el acceso al sistema de registro 2. Aplicar el instrumento de evaluación Lista de cheques basada en la NTP-ISO/IEC 17799:2007 3. Registrar los eventos identificados	1. Observación participativa, directa 2. Entrevista a los empleados y clientes 3. Acceso a los sistemas y bases de Datos 4. Revisión de documentos.	Humano: 2 personas Tecnológico: 1 PC, 1 Cámara Fotográfica Tiempo: 1 día	La Evaluación debe ser a los accesos lógicos que se tienen por parte de los usuarios a la información (DF)
DG002	- Evaluar una correcta Gestión de Privilegios.	1. Solicitar permiso para evaluar el Área encargada de la Actividad (Mesa De Ayuda) 2. Establecer fecha de Evaluación 3. Realizar la Evaluación de acuerdo al instrumento (lista de Chequeo)	1. Entrevista al personal encargado de la asignación de privilegios. 2. Pruebas al sistema. 3. Observación Directa	Humano: 2 personas Tecnológico: 1 PC, 1 Grabadora Tiempo: 1 día	Se debe Evaluar el proceso desde la delegación de privilegios a los usuarios.
DG003	Evaluar Los Reportes de Acceso	1. Solicitar acceso al sistema o banco de datos de donde se obtendrán los reportes. 2.Evaluar los reportes obtenidos en base a la NTP-ISO/IEC 17799:2007 3. Evaluar la documentación necesaria.	1. Pruebas al sistema 2. Revisión de reportes 3. Entrevista a los encargados	Humano: 1 Persona Tecnológico: 1 PC, 1 Grabadora de Voz Tiempo: 1 día	La Evaluación de los reportes se refiere a los físicos, como a los virtuales generados por el sistema.
DG004	Evaluar la realización del procedimiento documentado.	1. Solicitar documentación necesaria para Evaluación (flujos de trabajo, documentación sobre los procedimientos, etc). 2. Verificar con el personal en labor si se cumplen las actividades de acuerdo a los establecido.	1. Revisión de la documentación. 2. Entrevistas a empleados. 3. Observación Directa	Humano: 3 Personas Tecnológico: 01 Laptop, 01Cámara Fotográfica Tiempo: 2 días	Procedimiento documentado se refiere a que los procedimientos deben de realizarse tal y como están en los documentos(flujos de trabajo, etc)

14

- **Guia de auditoría para la evaluación del tratamiento de la información digital**

Guia de Auditoria para la evaluación del cumplimiento de la Conservación, respaldo y recuperación de los datos personales					
Propietario del documento: Equipo Auditor		Universidad Peruana Unión Área: Dirección General de Tecnologías de Información		Fecha:	Hoja 2 de 3
Ref.	Actividad que será evaluada	Procedimientos de auditoría	Herramientas que serán utilizadas	Recursos	Observaciones
DG005	Evaluar el control de seguridad en los ambientes que contienen datos	1. Solicitar la autorización para una inspección por parte del responsable del área donde se encuentren los sistemas o equipos donde se almacena la información. 2. Realizar la inspección de acuerdo a los requerimientos establecidos en la lista de chequeo. 3. Entrevistar a los encargados sobre los controles de seguridad establecidos. 4. Revisar la documentación requerida	Revision directa Experimentación en la seguridad física Revisión documental Entrevista a los empleados	Humano: 2 Personas Tecnológico: 1 Cámara Fotográfica. Tiempo: 1 a 2 días	El control de seguridad es físico. Se evaluará tanto la seguridad del acceso físico, así como la seguridad del ambiente donde se encuentran los sistemas que almacenan información
DG 006	Evaluar los mecanismos de respaldo de la información	1. Solicitar acceso a los respaldos de información. 2. Realizar pruebas de seguridad 3. Hacer revisiones especificadas en la lista de chequeo. 4. Evaluar al personal.	1. Realizacion de Pruebas al sistema. 2. Entrevista al personal. 3. Revision Documentaria.	Humano 1 a 2 Personas Tecnologico: 1 PC con acceso al sistema Tiempo: 1 a 2 días	Los mecanismos de respaldo pueden ser físicos como virtuales.

- **Guia de auditoría para la evaluación del tratamiento de la información digital**

Guia de Auditoria para la Evaluación de la Transferencia Logica o Electrónica de Datos Personales.					
Propietario del documento: Equipo Auditor		Universidad Peruana Unión Area: Dirección General de Tecnologías de Información		Fecha:	Hoja 5 de 5
Ref.	Actividad que será evaluada	Procedimientos de auditoría	Herramientas que serán utilizadas	Recursos	Observaciones
DG007	Supervisar la Autorización del Titular del BDP para la transferencia	1. Solicitar permisos para realizar las evaluaciones en el Área "(Dirección General) 2. Realizar la Evaluación sobre los requisitos establecidos en la Lista de Chequeo basados en la NTP-ISO/IEC 17799:2007 3. Revisar las evidencias necesarias.	1. Entrevista a los empleados- 2. Observación Directa 3. Revisión de Documentos	Humano: 1 persona Tecnológico: 1PC Tiempo: 1 día	Tomar mucha importancia a que ninguna transferencia se haga de no cumplir con los procedimientos de seguridad (Autorización)
DG 008	Revisar el Medio de transporte autorizado por el "BDP" para las transferencias	1. Realizar la evaluación del medio por el cual se enviar los datos de acuerdo los establecido por el titular 2. Evaluar los requerimientos de la lista de chequeo.	1. Revisión Documentaria. 2. Revisión Directa y participativa	Humano: 2 personas Tecnológico: 1PC Tiempo: 1 día	Los Medios de transporte se refieren a los medios por los cuales se están enviando la información, mensajes, correos, etc
DG 009	Revisar los Mecanismos de cifrado de Datos para la transferencias.	1. Solicitar acceso a los medios de transporte de la información. 2. Realizar pruebas para la evaluación de mecanismos de cifrado de datos. 3. Revisar en base a la Lista de chequeo los mecanismos de cifrado de Datos.	1. Pruebas de seguridad. 2. Revisión Directa y Participativa	Humano: 2 Personas Tecnológico: 1 PC, Software necesario Tiempo: 1 día	Los mecanismos de cifrado de datos que pueden utilizarse están nombrados en la NTP-ISO/IEC 17799:2007

15

10.1. Guía de la auditoría para la evaluación de la información no automatizada (Secretaría General)

- Guía de auditoría para la evaluación del almacenamiento, copia y acceso a la información no automatizada

Guía de Auditoría para la Evaluación del almacenamiento, copia y acceso a la información no automatizada					
Propietario del documento: Equipo Auditor		Universidad Peruana Unión Área: Dirección General de Tecnologías de Información		Fecha:	Hoja 1 de 3
Ref.	Actividad que será evaluada	Procedimientos de auditoría	Herramientas que serán utilizadas	Recursos	Observaciones
SG001	Almacenamiento de documentación no automatizada	1. Solicitar permisos al área de "Archivo institucional" para la evaluación 2. Realizar la Evaluación sobre los requisitos establecidos en la Lista de Chequeo basados en la NTP-ISO/IEC 17799:2007 3. Revisar las evidencias necesarias.	1. Entrevista a los empleados 2. Observación directa 3. Revisión de Documentos	Humano: 2 persona Tiempo: 1 día	Verificar quien lo hace y como realiza el almacenamiento
SG002	Copia o reproducción de la documentación no automatizada	1. Solicitar una reunión al personal para consultar el procesos de la copia y/o reproducción no automatizada 2. Evaluar los requerimientos de la lista de chequeo. 3. Revisar las evidencias necesarias.	1. Revisión documentaria. 2. Revisión directa y participativa 3. Entrevista a los empleados	Humano: 2 personas Tecnológico: Impresoras, PCS	Reconocer el motivo de la copia o reproducción, como también el encargado de la tarea
SG003	Acceso a la documentación no automatizada	1. Solicitar una reunión al personal para consultar el procesos de la copia y/o reproducción no automatizada 2. Evaluar los requerimientos de la lista de chequeo. 3. Revisar las evidencias necesarias.	1. Entrevista a los empleados 2. Observación directa 3. Realizar pruebas	Humano: 2 Personas Tiempo: 1 día	Verificar quien lo hace y como realiza el almacenamiento

- Guía de auditoría para la evaluación del traslado de la documentación no automatizada

Guía de Auditoría para la Evaluación del traslado de la documentación no automatizada					
Propietario del documento: Equipo Auditor		Universidad Peruana Unión Área: Dirección General de Tecnologías de Información		Fecha:	Hoja 2 de 3
Ref.	Actividad que será evaluada	Procedimientos de auditoría	Herramientas que serán utilizadas	Recursos	Observaciones
SG004	Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado	1. Solicitar una reunión al personal para consultar el procesos de la copia y/o reproducción no automatizada 2. Evaluar los requerimientos de la lista de chequeo. 3. Revisar las evidencias necesarias.	1. Entrevista a los empleados 2. Observación directa 3. Revisión de documentos	Humano: 2 persona Tiempo: 1 día	Comentar casos y/o experiencias con el personal en cuanto a los accesos
SG005	Eventos o incidentes en el traslado de datos personales	1. Solicitar una reunión al personal para consultar el procesos de la copia y/o reproducción no automatizada 2. Evaluar los requerimientos de la lista de chequeo. 3. Revisar las evidencias necesarias.	1. Entrevista a los empleados- 2. Observación directa 3. Revisión de documentos	Humano: 2 personas Tiempo: 2 día	Comentar casos y/o experiencias con el personal en cuanto a los accesos

16

Anexo 2. Lista de chequeo para la evaluación de Medidas de Seguridad en DIGETI

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

Área:	Fecha:
Auditor:	Cargo:
Auditado:	Cargo:

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

.Actividades a evaluar	ESCALA DE CUMPLIMIENTO			
		NO	PARCIAL	SI
1. Seguridad para el tratamiento de la Información Digital				
1.1. Evaluar el control de acceso a la información				
1.1.1. ¿El Sistema Académico está protegido contra el acceso lógico no autorizado?		0	1	2
1.1.2. ¿Se utilizan ID's únicos para dar acceso a los usuarios del Sistema Académico?		0	1	2
1.1.3. ¿El servidor del sistema almacena contraseñas de inicio de sesión de manera cifrada?		0	1	2
1.1.4. ¿Se permite que el usuario cambie la contraseña cuando lo desee?		0	1	2
1.1.5. Para la creación de un nuevo usuario (Alumnos, Docentes, Administrativos)¿se revisa que el usuario tenga la autorización dada por el propietario del banco de datos?		0	1	2
1.1.6. ¿Se requiere que las contraseñas contengan al menos 8 dígitos, números y al menos incluyan un carácter especial?		0	1	2
1.1.7. Para la creación de un nuevo usuario (Alumnos, docentes, administrativos): ¿Revisa que el nivel otorgado sea apropiado para el propósito?		0	1	2
1.1.8. Durante la creación de un nuevo usuario: ¿Se le proporciona a los usuarios un documento escrito de sus derechos de acceso?		0	1	2
1.1.9. Para la creación de un nuevo usuario: ¿Se requiere a los usuarios la firma de un documento indicando el entendimiento de las condiciones de acceso?		0	1	2
1.1.10. ¿DIGETI, se asegura que no se proporcione el acceso hasta haber completado los procedimientos de autorización?		0	1	2
1.1.11. ¿Se mantiene un registro formal de todas las personas registradas para usar el servicio?		1	2	3
1.1.12. ¿Se verifica la eliminación o bloqueo inmediato de los derechos de acceso a los		0	1	2

usuarios que han cambiado de puesto o han dejado la organización?				
1.1.13. ¿Se asegura que no se emitan ID's redundantes a otros usuarios?		0	1	2
1.1.14. ¿Se realiza un chequeo periódico para eliminar o bloquear los ID's de usuario o cuentas redundantes?		0	1	2
1.2. Evaluar una correcta gestión de privilegios		**NO**	**PARCIAL**	**SI**
1.2.1. ¿Se cuentan con políticas donde se regule la disposición de privilegios al sistema?		0	1	2
1.2.2. ¿Se tiene un proceso de autorización debidamente documentado?		0	1	2
1.2.3. ¿Se otorga privilegios de acuerdo a la necesidad basándose las políticas de control de acceso?		0	1	2
1.2.4. ¿Se mantiene un registro de todos los privilegios asignados a los usuarios?		0	1	2
1.2.5. ¿Se verifica que no se otorguen privilegios hasta completar el proceso de autorización?		0	1	2
1.2.6. ¿Los privilegios se asignan a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio?		0	1	2
1.2.7. ¿Se revisan las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados?		0	1	2
1.2.8. ¿Se revisan las autorizaciones para los usuarios con privilegios especiales en intervalos de tiempo más cortos?		0	1	2
1.3. Evaluar los reportes de accesos		**NO**	**PARCIAL**	**SI**
1.3.1. ¿Se generan y mantienen registros que provean evidencia de accesos al sistema?		0	1	2
1.3.2. ¿Hay trazabilidad en los registros de acceso al sistema, como: horas de inicio, cierre de sesión y acciones relevantes?		0	1	2
1.4. Evaluar la realización del procedimiento documentado		**NO**	**PARCIAL**	**SI**
1.4.1. ¿Se cuenta con flujos de trabajos o procedimientos establecidos para el control de accesos?		0	1	2
1.4.2. ¿Se realizan las actividades de acuerdo a los procedimientos documentados?		0	1	2
1.4.3. ¿Se realizan auditorias de cumplimiento del control de accesos establecidos en la directiva de seguridad de la información de banco de datos personales?		0	1	2

Actividades a evaluar		ESCALA DE CUMPLIMIENTO			
		Peso:	NO	PARCIAL	SI
2. Conservación, respaldo y recuperación de Datos Personales					
2.1 Evaluar el control de seguridad en los ambientes que contienen datos					
2.1.1	¿Los perímetros del edificio o local que contienen los medios de almacenamiento de Información son físicamente solidos?		0	1	2
2.1.2	¿Las puertas y ventanas están protegidas de accesos no autorizados por mecanismos de control: Por ejemplo vallas, alarmas , relojes, etc.		0	1	2
2.1.3	¿Los medios de almacenamiento de Información se encuentran físicamente separados de aquellos ajenos a la organización?		0	1	2
2.1.4	¿Se usan controles de autenticación para restringir el acceso a los ambientes de procesamiento y almacenamiento de Información personal?		0	1	2
2.1.5	EL personal de servicios de ajenos al área ¿cuenta con acceso restringido a las áreas seguras o los medios de procesamiento de Información Personal?		0	1	2
2.2 Evaluar los Mecanismos de respaldo de la información			**NO**	**PARCIAL**	**SI**
2.2.1	¿Se mantienen copias de seguridad del banco de datos personales?		0	1	2
2.2.2	¿Las copias de respaldo de datos personales son protegidas mediante técnicas de cifrado?		0	1	2
2.2.3	¿Las copias de respaldo se almacenan en un lugar físicamente apartado del local principal, para evitar algún daño por algún accidente o desastre natural?		0	1	2
2.2.4	La Información de respaldo cuenta con el mismo nivel de seguridad física y ambiental que el local principal.		0	1	2
2.2.5	¿Los medios de respaldos se prueban regularmente para comprobar su correcto funcionamiento?		0	1	2
2.3 Evaluar procedimientos de restauración de respaldos.			**NO**	**PARCIAL**	**SI**
2.3.1	¿Los procedimientos de restauración se chequean y prueban regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación?		0	1	2
2.3.2	¿Las pruebas realizadas a los respaldos cuentan con la documentación adecuada?(fecha y hora de la prueba, nombre del que realizo, BDP recuperado, tiempo de recuperación, resultados de la pruebas)		0	1	2
2.3.3	¿Se toman acciones en caso de pruebas insatisfactorias?		0	1	2

2.3.4 Cuando se restaura una copia de seguridad del banco de datos personales ¿se requiere autorización del titular de BDP o quien es te asignado?		0	1	2
Actividades a evaluar	**Peso:**	**ESCALA DE CUMPLIMIENTO** **NO**	**PARCIAL**	**SI**
3. Transferencia lógica o electrónica de Datos Personales.				
3.1. Supervisar la autorización del titular del BDP para la transferencia.				
3.1.1. Se cuentan con políticas para la transferencia lógica o electrónica de Datos Personales		0	1	2
3.1.2. ¿El tratamiento de datos personales es autorizado por el titular del banco de datos personales?		0	1	2
3.1.3. **¿**Se cuenta con algún documento que garantice la trasferencia Internacional de Datos Personales?		0	1	2
3.1.4. **¿**Se procede a la transferencia Datos Personales aun sin la autorización previa del Titular de Banco de Datos o encargado?		0	1	2
3.2. Medios de transporte para la transferencia de datos personales.		**NO**	**PARCIAL**	**SI**
3.2.1. ¿Se cuentan con medios de envío autorizados Titular de BDP para la trasferencia de Datos?		0	1	2
3.2.2. ¿Se controla el uso de los medios de transferencia de datos personales?		0	1	2
3.2.3. ¿Existe evidencia documentada del uso de los medios de transferencia establecidos?		0	1	2
3.2.4. ¿Se utilizan software especializado para la transferencia de datos personales?		0	1	2
3.3. **Mecanismos de Seguridad en la transferencia de Datos Personales**				
3.3.1. ¿Se encuentran establecidos los mecanismos de seguridad para la transferencia en las políticas?		0	1	2
3.3.2. ¿Los equipos utilizados para la transferencia lógica cuentan con software de protección contra códigos maliciosos?		0	1	2
3.3.3. ¿Se utilizan protocolos de comunicación cifrados como: VPN, correo electrónico cifrado, FTP seguro, otros?|		0	1	2
3.3.4. Los datos contenidos en soporte informático ¿se transportan previa encriptación y un mecanismo de verificación de la integridad?		0	1	2
3.3.5. ¿El Área de tratamiento de datos personales tiene restringido el uso de herramientas de registro no autorizadas? (cámara de video, fotográficas, grabación de audio, etc.)		0	1	2

4. Prestación de servicios sin acceso a datos personales				
4.1. Servicios internos de la organización o área sin acceso a datos personales				
4.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		0	1	2
4.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		0	1	2
4.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		0	1	2
4.1.4. ¿Se generan documentos mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		0	1	2
4.2. Servicios externos a la organización sin acceso a datos personales		**NO**	**PARCIAL**	**SI**
4.2.1. ¿Se generan contratos expresos o cláusulas contractuales sobre el tratamiento de datos personales al momento de prestar servicios externos?		0	1	2
4.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?		0	1	2
4.2.3. ¿Existe algún documento que garantice la destrucción o imposibilidad de recuperación de los datos alojados en el servicio del prestador de servicio una vez concluida la relación con el proveedor?		0	1	2
4.2.4. ¿Se realizan visitas a la infraestructura del proveedor para comprobar el cumplimiento del servicio? O en caso de un proveedor extranjero: ¿Los prestadores de servicio cuentan con reportes SOC para verificar el cumplimiento del servicio?		0	1	2

X _____
Auditor Externo

X _____
Encargado Área Auditada

X _____
Director de DIGETI

Anexo 3. Lista de chequeo para la evaluación de Medidas de Seguridad en Secretaría General

EVALUACIÓN DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

Área:	Fecha:
Auditor:	Cargo:
Auditado:	Cargo:

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada			
1.1. Almacenamiento de documentación no automatizada			
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.	1	2	3
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?	1	2	3
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?	1	2	3
1.2. Copia o reproducción de la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?	1	2	3
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? Sin permitir su recuperación.	1	2	3
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?	1	2	3
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos	1	2	3
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?	1	2	3
1.3. Acceso a la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.3.1 ¿Se cuenta con algún documento donde indique la responsabilidad que recae en el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos?	1	2	3

Página **1** de **3**

EVALUACIÓN DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

1.3.2 ¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?		1	2	3
1.3.3 ¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?		1	2	3
1.3.4 ¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?		1	2	3

Actividades a evaluar		ESCALA DE CUMPLIMIENTO		
		NO	PARCIAL	SI
2. Traslado de la documentación no automatizada				
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado				
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?		1	2	3
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?		1	2	3
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?		1	2	3
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?		1	2	3
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?		1	2	3
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?		1	2	3
2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.		1	2	3
2.2. Eventos o incidentes en el traslado de datos personales		**NO**	**PARCIAL**	**SI**
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?		1	2	3

2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?		1	2	3
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?		1	2	3

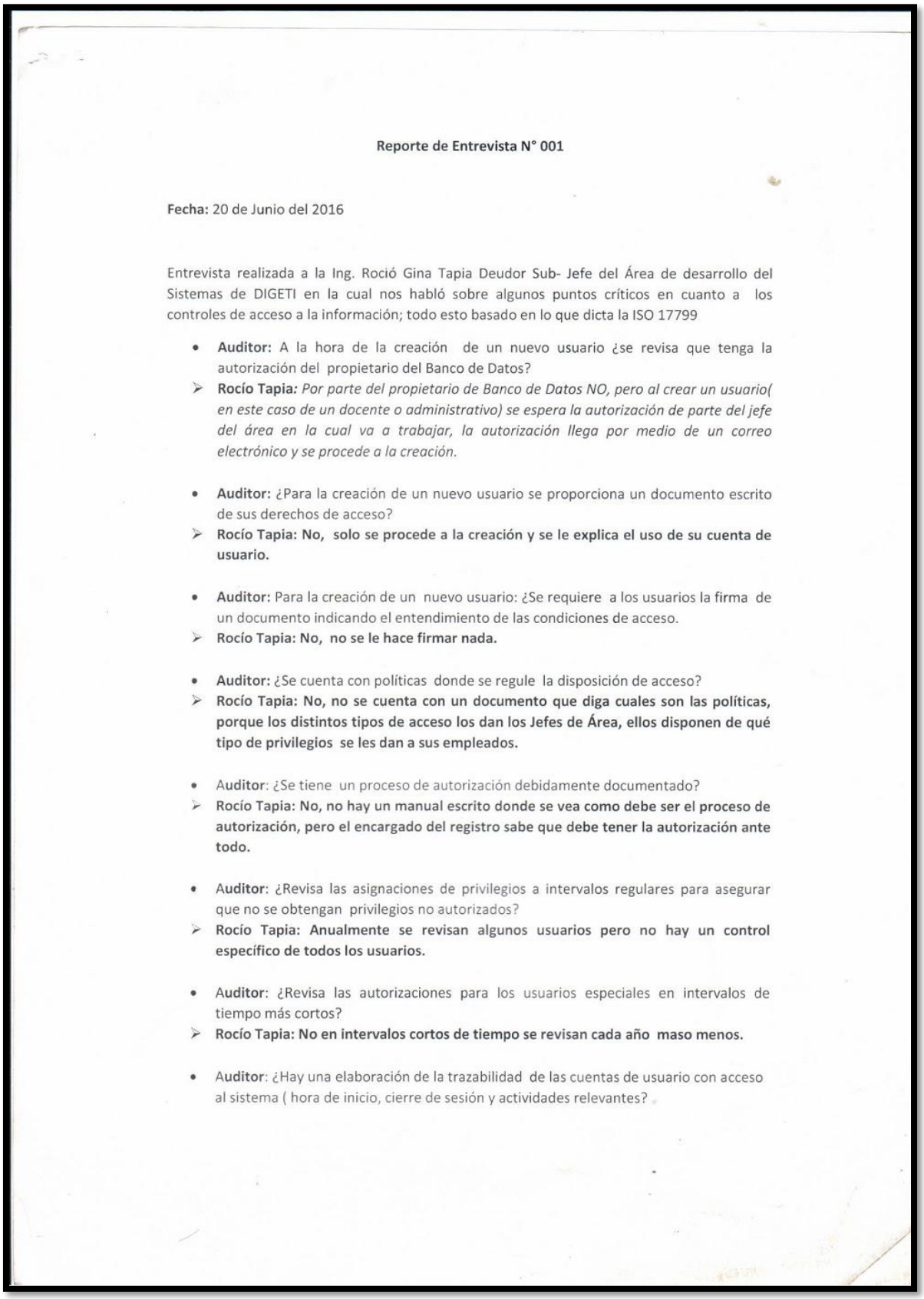
Actividades a evaluar	ESCALA DE CUMPLIMIENTO			
		NO	PARCIAL	SI
3. Prestación de servicios sin acceso a datos personales				
3.1. Servicios internos de la organización o área sin acceso a datos personales				
3.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		1	2	3
3.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		1	2	3
3.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		1	2	3
3.1.4. ¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		1	2	3
3.2. Servicios externos a la organización sin acceso a datos personales		**NO**	**PARCIAL**	**SI**
3.2.1. ¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?		1	2	3
3.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?		1	2	3
3.2.3. ¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?		1	2	3

X _____
Auditor Externo

X _____
Encargado Área Auditada

X _____
Secretario General

Anexo 4. Evidencias del análisis GAP en DIGETI



Reporte de Entrevista N° 001

Fecha: 20 de Junio del 2016

Entrevista realizada a la Ing. Roció Gina Tapia Deudor Sub- Jefe del Área de desarrollo del Sistemas de DIGETI en la cual nos habló sobre algunos puntos críticos en cuanto a los controles de acceso a la información; todo esto basado en lo que dicta la ISO 17799

- **Auditor:** A la hora de la creación de un nuevo usuario ¿se revisa que tenga la autorización del propietario del Banco de Datos?
  - **Rocío Tapia:** *Por parte del propietario de Banco de Datos NO, pero al crear un usuario(en este caso de un docente o administrativo) se espera la autorización de parte del jefe del área en la cual va a trabajar, la autorización llega por medio de un correo electrónico y se procede a la creación.*

- **Auditor:** ¿Para la creación de un nuevo usuario se proporciona un documento escrito de sus derechos de acceso?
  - **Rocío Tapia: No, solo se procede a la creación y se le explica el uso de su cuenta de usuario.**

- **Auditor:** Para la creación de un nuevo usuario: ¿Se requiere a los usuarios la firma de un documento indicando el entendimiento de las condiciones de acceso.
  - **Rocío Tapia: No, no se le hace firmar nada.**

- **Auditor:** ¿Se cuenta con políticas donde se regule la disposición de acceso?
  - **Rocío Tapia: No, no se cuenta con un documento que diga cuales son las políticas, porque los distintos tipos de acceso los dan los Jefes de Área, ellos disponen de qué tipo de privilegios se les dan a sus empleados.**

- **Auditor**: ¿Se tiene un proceso de autorización debidamente documentado?
  - **Rocío Tapia: No, no hay un manual escrito donde se vea como debe ser el proceso de autorización, pero el encargado del registro sabe que debe tener la autorización ante todo.**

- **Auditor**: ¿Revisa las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados?
  - **Rocío Tapia: Anualmente se revisan algunos usuarios pero no hay un control específico de todos los usuarios.**

- **Auditor**: ¿Revisa las autorizaciones para los usuarios especiales en intervalos de tiempo más cortos?
  - **Rocío Tapia: No en intervalos cortos de tiempo se revisan cada año maso menos.**

- **Auditor**: ¿Hay una elaboración de la trazabilidad de las cuentas de usuario con acceso al sistema (hora de inicio, cierre de sesión y actividades relevantes?

- **Rocío Tapia: El sistema si registra las horas de acceso al sistema y las horas de desconexión, así como las veces que inicio ; pero no cuenta con un registro de las actividades realizadas por cada usuario.**

- **Auditor**: ¿Cuenta con flujos de trabajo establecidos para el control de accesos?
- **Rocío Tapia: No, no tenemos flujos de trabajo documentados.**

- **Auditor**: ¿Se realizan actividades de acuerdo a lo documentado?
- **Rocío Tapia: No.**

- **Auditor**: ¿Se realizan auditorias sobre el cumplimiento del control de accesos establecidos en la directiva de Seguridad de la información del Banco de Datos Personales?
- **Rocío Tapia: No, no se han realizado auditorias para lo que es registro, o los controles de acceso, en otras áreas si pero aquí no.**

X

Rocio Tapia
Sub-Jefe de Desarrollo

DOCUMENTO DE RESPALDO

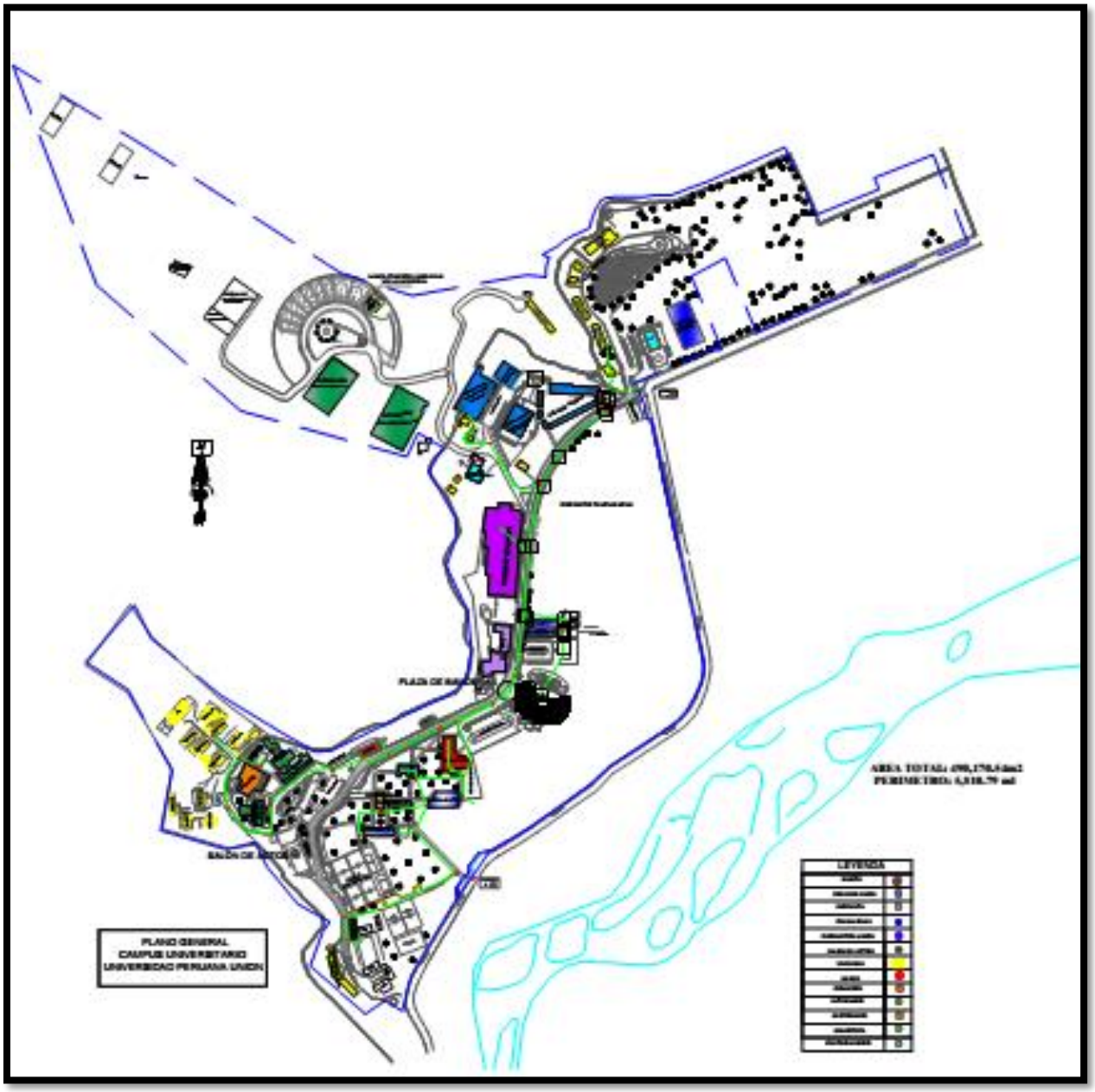
Yo Immer Elías Cuellar Rodríguez identificado con DNI 40969219, Director del área DIGETI.
Después de haber tenido una evaluación de auditoria sobre el "Cumplimiento de medidas de seguridad de la Ley N° 29733", me corresponde afirmar en el presente documento el incumplimiento en algunos aspectos de la evaluación. Con la finalidad de poder cumplir con la LPDP, la continuidad del negocio y garantizar el derecho fundamental a la protección de datos personales a nuestros usuarios.

Lista de irregularidades (NO SE CUMPLE):

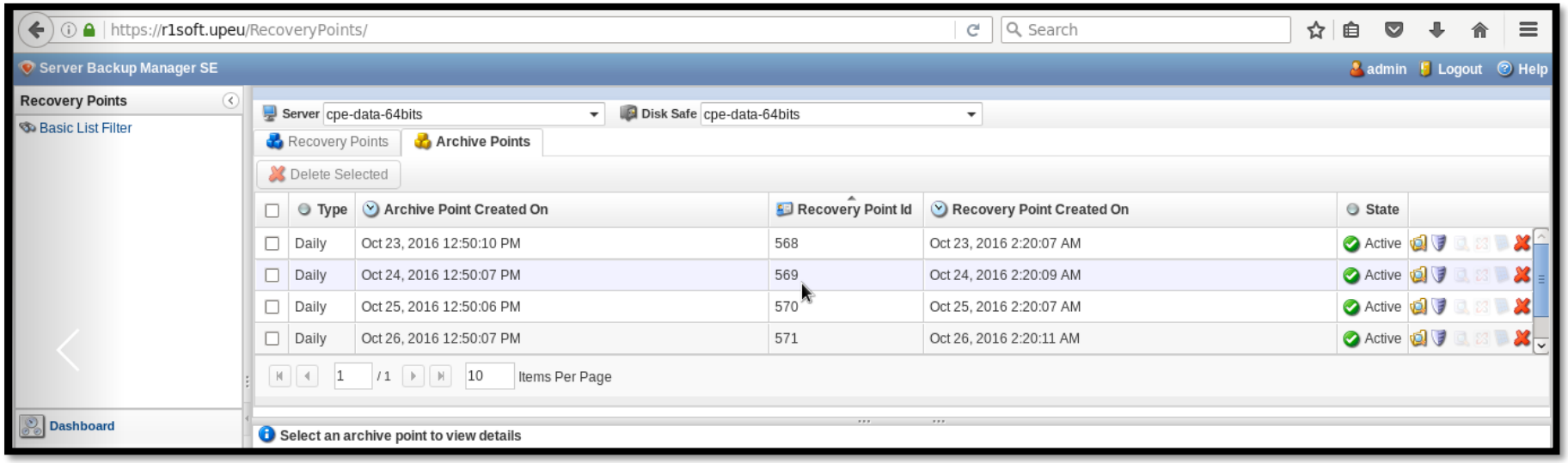
1. No se cumple con políticas de transferencia lógicas y no se han establecido mecanismos
2. No se cuenta con un documento de seguridad que garantice la transferencia nacional e internacional
3. No existe evidencia documentada del uso de medios de transferencia
4. No se cumple con el uso de software especializado para la transferencia
5. No cumple con la inscripción previa al envío de datos personales y no el Control de los medios de Transf.
6. No cumple con el aseguramiento a la integridad y confidencialidad en la transferencia de los datos pers.
7. No se cumple con el uso restringido de herramientas no autorizadas al área donde se tratan los datos pers.

FIRMA

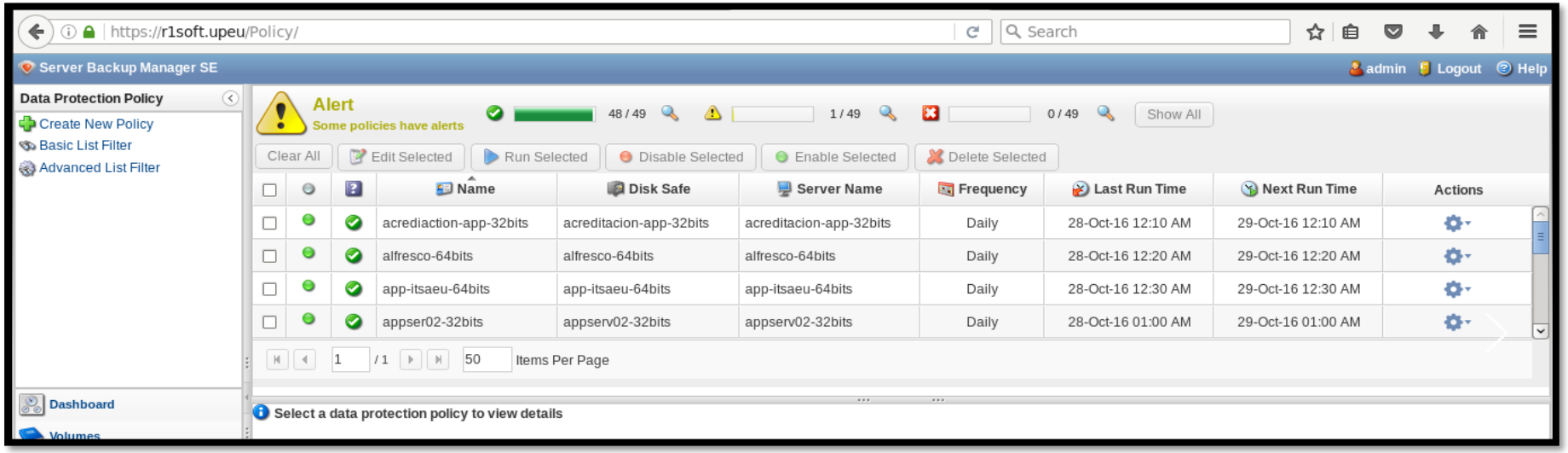
Plano de instalación Fibra en la UPeU



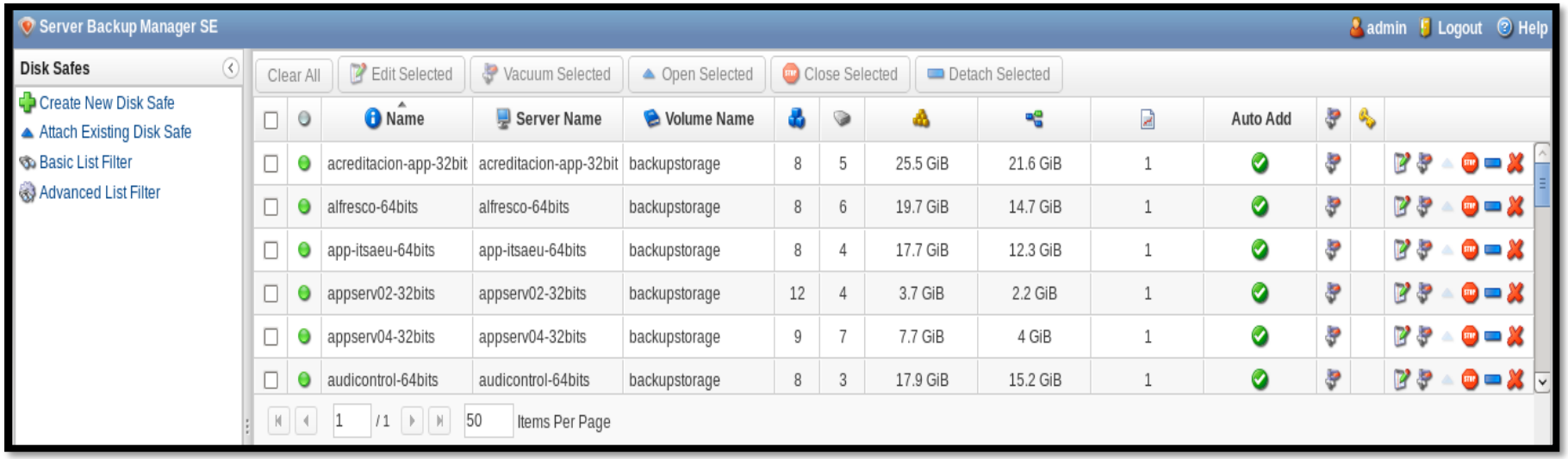
Política de punto de recuperación



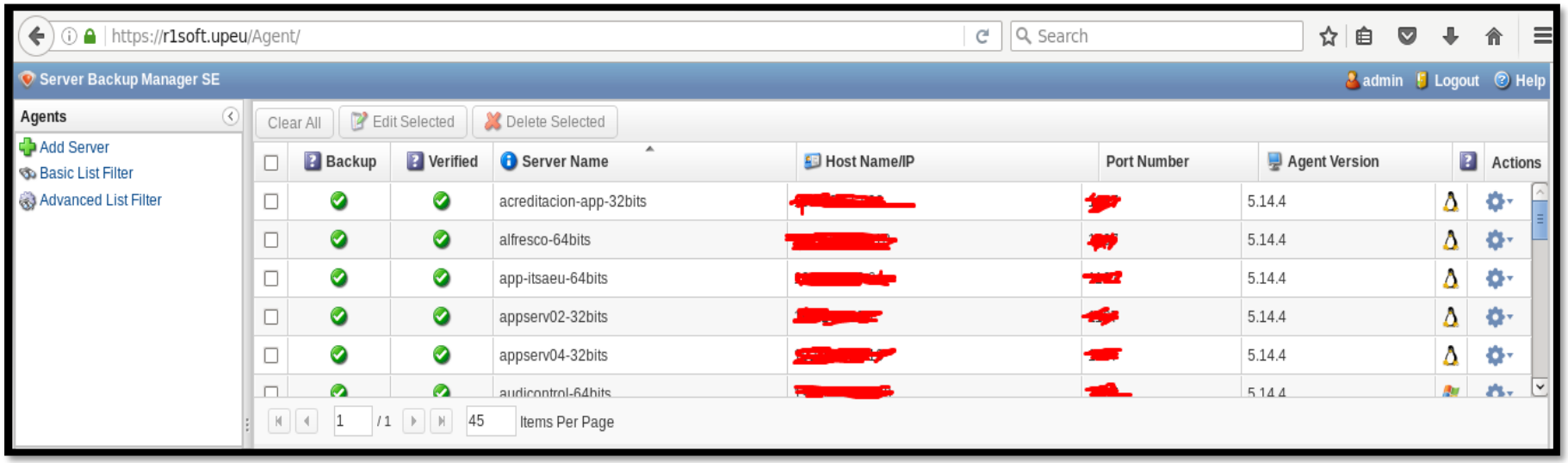
Política de horario de backups



Política de discos a recuperar

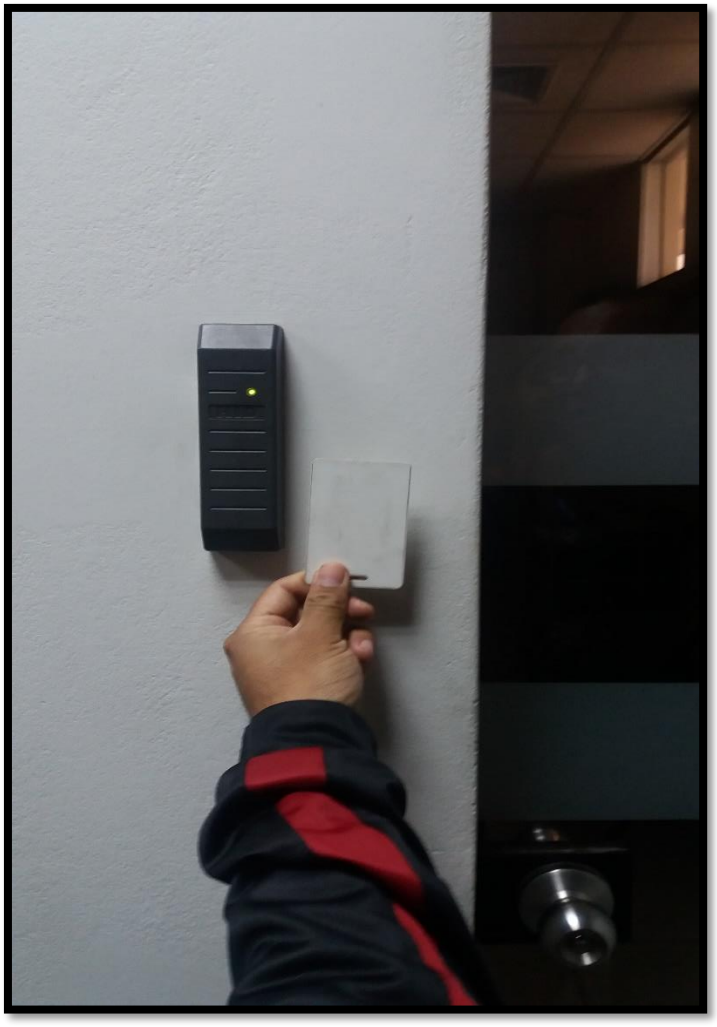


Servidores de backups



Tecnología para el acceso al data center y alarma contra incendios

Autenticación para el data center

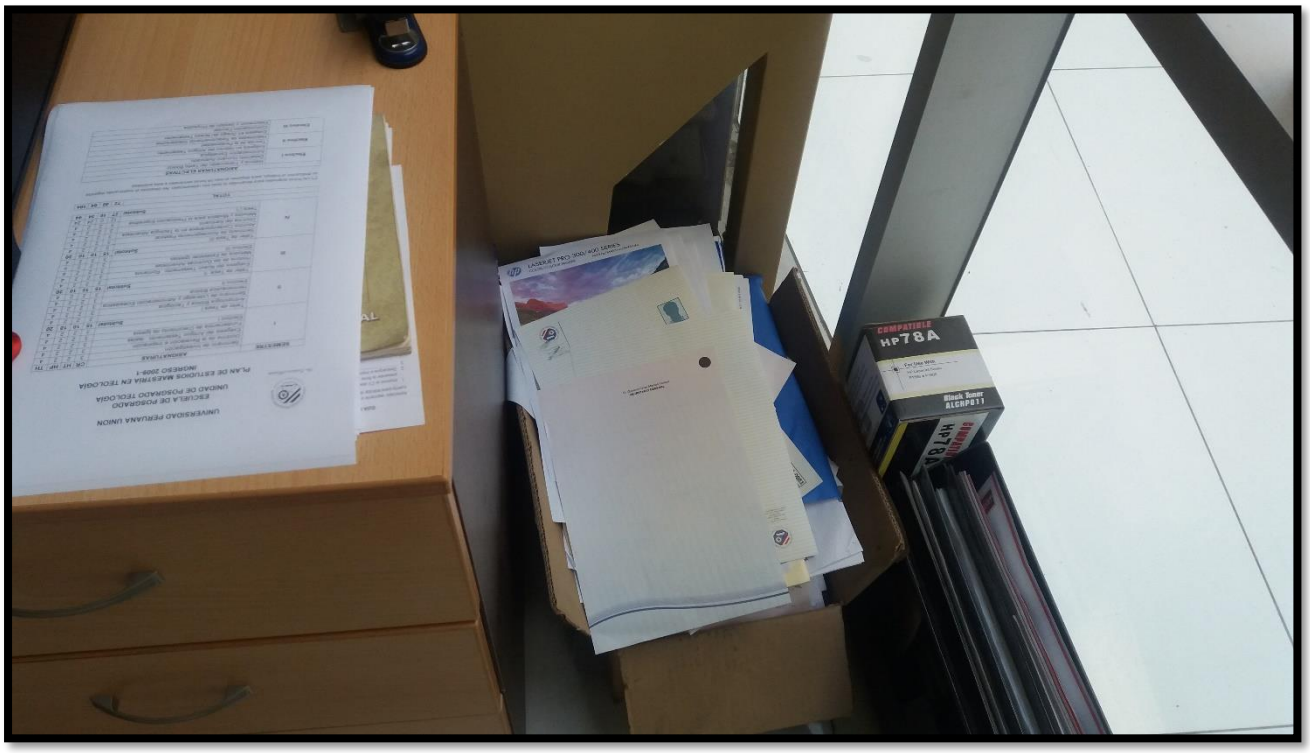


Anexo 5. Evidencias del análisis GAP en Secretaría General

Puerta del “Archivo académico general” en condición vulnerable

Sobre para transferir documentos

Documentos con datos personales expuestos



Dispositivo 1 para realizar copias a documentos que contienen datos personales

Dispositivo 2 para realizar copias a documentos que contienen datos personales

Dispositivo 3 para realizar copias a documentos que contienen datos personales

Dispositivo 4 para realizar copias a documentos que contienen datos personales

Anexo 6. Informe de Dictamen final de auditoría para Secretaría General y DIGETI

Lima, 30 de enero del 2018

Señor:
Abog. Wilberth Gonzales Taco
Secretario General

Me permito remitir a usted el informe final de resultados de la auditoría realizada al área de Secretaria General de la Universidad Peruana Unión, que se realizó del 13 de octubre al 01 de Noviembre del 2016.

La revisión realizada se basó en los Artículos 42: Almacenamiento de documentación no automatizada, Articulo 43: Copia y reproducción de documentación no automatizada, Articulo 44: Acceso a la documentación y Articulo 45: Traslado de documentación no Automatizada; del Título V "Medidas de Seguridad" del Reglamento de la Ley de Protección de Datos Personales

El citado informe encontrará el dictamen y las conclusiones a las cuales se llegaron después de la aplicación de la auditoría.

Quedo de usted para cualquier aclaración al respecto.

Atentamente,

Cristhian Calisaya Sana
Jefe del Proyecto de Auditoria.

Lima, 13 de Enero de 2017

Señor:
Mg. Elías Cuellar Rodríguez
Director General DIGETI

Me permito remitir a usted el informe final de resultados de la auditoría realizada a la Dirección General de Tecnologías de Información de la Universidad Peruana Unión, que se realizó del 20 de Septiembre al 15 de Octubre del 2016.

La revisión realizada se basó en los Artículos 39: Seguridad y tratamiento de información digital, Artículo 40: Conservación, respaldo y recuperación de datos personales y el Artículo 41: Transferencia lógica o electrónica de los datos personales; del Título V "Medidas de Seguridad" del Reglamento de la Ley de Protección de Datos Personales.

El citado informe encontrará el dictamen y las conclusiones a las cuales se llegaron después de la aplicación de la auditoría.

Quedo de usted para cualquier aclaración al respecto.

Atentamente,

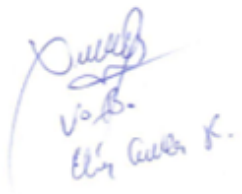
Cristhian Calisaya Sana
Jefe del Proyecto de Auditoria.

INFORME FINAL DE AUDITORÍA

Empresa auditada	UNIVERSIDAD PERUANA UNION – SECRERTARÍA GENERAL
Objeto de auditoria	Evaluar el cumplimiento de la Ley Nro. 29733 en la Universidad Peruana Unión
Dirigido a	Abog. Wilberth Gonzales Taco
Fecha del Informe Final	31/01/2018
Responsables	Cristhian Calisaya Sana; Milton Tarrillo Villegas

INFORME FINAL DE AUDITORÍA

Empresa auditada	UNIVERSIDAD PERUANA UNION – DIRECCION DE TECNOLOGIAS DE INFORMACION
Objeto de auditoria	Evaluar el cumplimiento de la Ley Nro. 29733 en la Universidad Peruana Unión
Dirigido a	Immer Elías Cuellar Rodríguez
Fecha del Informe Final	13/01/2017
Responsables	Cristhian Calisaya Sana; Milton Tarrillo Villegas



1. INTRODUCCIÓN

1.1. Objetivos de la Auditoría

Evaluar el cumplimiento de la Ley Nro 29733 "Ley de protección de Datos Personales" en los procesos de la Universidad Peruana Unión, con el objetivo de reconocer el estado actual de la organización y ver la deficiencias actuales para lograr su cumplimiento generando la continuidad del negocio y garantizado el derecho fundamental a la protección de datos personales. Evitando sanciones y/o multas por el incumplimiento por parte de la ANPDP.

1.2. Alcance y limitaciones

1.2.1. Alcance

EL alcance de la auditoría es la evaluación del cumplimiento del Artículo 16: Seguridad del tratamiento de la Ley de Protección de Datos Personales; así como en su Reglamento en su Capítulo V" Medidas de Seguridad", tomando como referencia para el cumplimiento los controles 9.-Seguridad Física y ambiental; 10.- Gestión de las comunicaciones y operaciones y 11.- Control de acceso de la NTP-ISO/IEC 17799:2007 Código de buenas prácticas para la gestión de la Seguridad de la Información.

1.2.2. Limitaciones

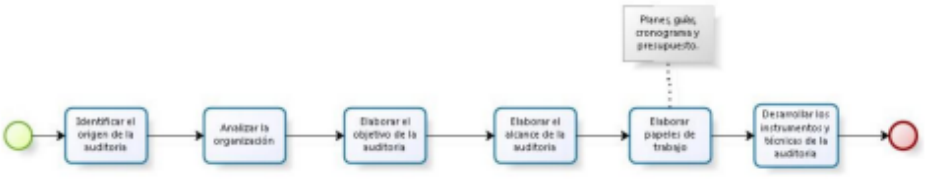
La evaluación se limita solo en el cumplimiento del "Principio de Seguridad" que es uno de los principios rectores de la Ley de Protección de Datos Personales, donde nos señala que se deben optar medidas técnicas, organizativas y legales para garantizar la seguridad de los Datos Personales.

1.2.3. Periodo y Actividades

El periodo de la auditoría abarcó los meses de Septiembre, Octubre y Noviembre y del 2016.

Planificar

En los meses de , se llevó a cabo la planificación de la Auditoría donde se identificaron las áreas de la organización donde se llevarían se realizaría la etapa de Ejecución de Auditoria, además de realizaron actividades como: Realizar visitas preliminares, definir objetivos, estudiar el contexto de la organización y área, definir el alcance y límites de la auditoría, elaborar instrumentos de trabajo, etc. *Ver Figura1.*

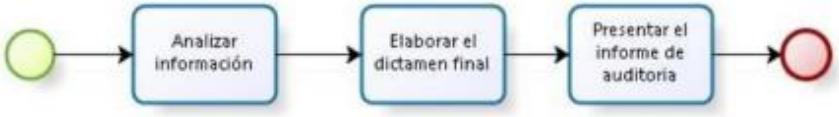


Ejecutar

Se desarrolló en el mes de Noviembre, se precedió con la Ejecución de la Auditoría, las actividades realizadas con este periodo fue ejecutar las actividades planificadas, controlar el avance del equipo auditor, aplicar los instrumentos, obtener evidencias y desviaciones, analizar las evidencias e integrar los papeles obtenidos durante el tiempo de ejecución.

Elaboración de Dictamen Final.

Una vez obtenida la información de la evaluación y las evidencias de las desviaciones, se procedió con la última etapa que es el Dictamen Final, en la que desarrollaron las siguientes actividades: Análisis de la Información, elaboración del dictamen final y la presentación del informe de auditoría.



1.3. Metodología y procedimientos de auditoria

1.3.1. Metodología para Auditorias de Sistemas Computaciones.

La metodología aplicada en el presente proyecto es la de "Auditorías para sistemas Computacionales", que contempla 3 etapas.

1.3.2. Instrumentos utilizadas para la recopilación de datos:

Los instrumentos utilizados durante la recopilación son:

1.3.2.1. Entrevista:

Durante las visitas a las áreas de DIGETI y Sec. General se utilizaron entrevistas libres dirigidas, de comprobación e informales, Estas entrevistas de se hicieron a los encargados de cada área.

Se iniciaba con la presentación de cada integrante del equipo auditor, y luego el auditor principal procedía a dar una breve explicación de la auditoria y su finalidad.
Respetando los tiempos del auditado se avanzaban con las preguntas, y se prestaban notas de preguntas adicionales que surgían fuera del instrumento; se procedía a tomar evidencias de las no conformidades, (fotos, videos, registro de pruebas), antes de cerrar con la entrevista se daba un pequeño tiempo para cubrir algún interrogante o duda del auditado. Al culminar la entrevista se agradecía por el tiempo invertido y dependiendo del caso se quedaba para una próxima entrevista.

1.3.2.2. Encuestas

Para la presente auditoria se desarrollaron dos (02) "Check List" para la recopilación de información. Este tipo de encuesta fue de forma específica y con preguntas precisas las cuales nos permitieron analizar e interpretar la información de una mejor manera.

1.4. Breve descripción del contenido del informe

El presente se delegaron responsabilidades a los miembros del equipo, se contó con la colaboración de las áreas de DIGETI y Sec. General, para ejecutar las auditorías y recabar las evidencias y el llenado de las listas de chequeo (Check List)
La obtención de las evidencias fueron mediante, fotos de ser el caso, registros de pruebas al sistema, para comprobar la funcionalidad que se requiera.
Los resultados se especifican por cada lista de chequeo y al final se muestra un balance total de los resultados, así mismo se muestran las recomendaciones para las "no conformidades" basadas en la ISO/IEC NTP 17799:2007, el reglamento de la Ley de Protección de Datos Personales, (LPDP), así como sus Directivas de Seguridad.

2. PRESENTACIÓN DEL DICTAMEN (DIGETI)

2.1. Breve introducción al dictamen

2.2. Área de auditoría: Seguridad del Tratamiento de la Información Digital

2.2.1. Datos de Evaluación:

Área: Desarrollo de Sistemas.
Fecha:
Responsable: Cristhian Calisaya Sana
Apoyo: Milton Tarrillo
Instrumentos:

- Lista de Chequeo (basados en los requerimientos del Reglamento de la Ley y la ISO en cuanto a medidas de Control de Acceso)
- Documento de Registro de Hallazgos
- ISO 17799:2007
- 1 Pc para pruebas y verificaciones.
- Cámara Fotográfica.

Duración de la entrevista: 120 min aprox.

2.2.2. Descripción de las desviaciones encontradas.

- ✓ Inexistente función de bloqueo de usuario luego de 5 intentos de autenticación fallidos. (CH-001)
- ✓ Inapropiados requisitos para la creación de contraseñas. (CH-002)
- ✓ Inexistente documento de los derechos de acceso a usuarios (CH-003)
- ✓ Inexistente documento de entendimiento de las condiciones de acceso para los usuarios. (CH-004)
- ✓ Inexistente registro formal de personas registradas al sistema (CH-005)
- ✓ Deficiente eliminación y bloqueo de usuarios que dejan la organización (CH-006)
- ✓ Inexistentes políticas para la disposición de privilegios. (CH-007)
- ✓ Inexistente documentación sobre el proceso de autorización (CH-008)
- ✓ Inexistente revisión de usuarios para evitar privilegios no autorizados. (CH-009)
- ✓ Deficiente revisión en las asignaciones de privilegios y autorizaciones en usuarios con privilegios especiales. (CH-010)
- ✓ Incompleta información en los reportes de acceso. (CH-011)
- ✓ Inexistentes flujos de trabajo o procedimientos establecidos y documentados en la gestión de acceso. e Inadecuada realización de actividades de acuerdo a lo documentado.(CH-012)
- ✓ No garantizada realización de auditorías para el control de accesos. (CH-013)
- ✓ Inexistentes auditorias para el control de la Protección de Datos Personales. (CH-014)

2.3. Área de Auditoria: **Conservación, respaldo y recuperación de Datos Personales.**

2.3.1. Datos de Evaluación:

Área: Redes y Conectividad.

Fecha:

Responsable: Cristhian Calisaya Sana

Apoyo: Milton Tarrillo Villegas

Instrumentos:

- Lista de Chequeo (elaborada en base a los requerimientos del Control de Seguridad Física y Ambiental de la ISO 17799)
- Documento de Registro de Hallazgos
- 1 Cámara Fotográfica
- ISO 17799

Duración de la entrevista: 90min aprox.

2.3.2. Descripción de las desviaciones encontradas.

- ✓ Inadecuado lugar de almacenamiento de los medios de procesamiento de datos. (CH-015)
- ✓ Deficiente control del autenticación para el control de acceso al área de procesamiento de Datos información. (CH-016)
- ✓ Copias de respaldo sin técnicas de cifrado.(CH-017)
- ✓ Inadecuado lugar de almacenamiento físico de las copias de seguridad. (CH-018)
- ✓ Inadecuadas medidas de seguridad física del ambiente que contiene copias de seguridad. (CH-019)
- ✓ Deficiente información de pruebas a las copias de respaldo. (CH-020)

2.4. Área de Auditoria: **Conservación, respaldo y recuperación de Datos Personales.**

2.4.1. Datos de Evaluación:

Área: Redes y Conectividad.

Fecha:

Responsable: Cristhian Calisaya Sana

Apoyo: Milton Tarrillo Villegas

Instrumentos:

- *Lista de Chequeo (en base a los requerimientos de la ISO en cuanto a las medidas de control de acceso al sistema)*
- *Documento de Registro de Hallazgo.*
- *Reporte de entrevista*
- *ISO 17799, LPDP y RLPDP.*
- *1 PC para realizar pruebas y verificaciones.*

Duración de la entrevista: 90min aprox.

2.4.2. Descripción de las desviaciones encontradas.

- ✓ Políticas inexistentes para la transferencia lógica de los datos personales.
- ✓ Documentos inexistentes que garantice la transferencia nacional interna y externa de los datos personales.
- ✓ Incumplimiento de políticas de transferencia que detallen los medios de transporte para cualquier tipo de transferencia de datos personales.
- ✓ Incumplimiento de políticas de transferencia que detallen los medios de transporte para cualquier tipo de transferencia de datos personales.
- ✓ Software especializado inexistente para la transferencia de datos personales
- ✓ No se encuentran establecidos los mecanismos de seguridad en las políticas.

- ✓ No se encuentran establecidos los mecanismos de seguridad en las políticas.
- ✓ No se garantiza la integridad y confidencialidad cuando la información lógica es transmitida.
- ✓ Incumplimiento de encriptación previo al envío
- ✓ Inexistente evidencia del uso de técnicas para validar la identidad en los envíos digitales
- ✓ El uso de herramientas de registro no autorizadas (Cámara de video, , fotos, grabación, etc.) no están restringidos.

2.5. Área de Auditoria: **Prestaciones de servicios sin acceso a datos personales.**

2.5.1. Datos de Evaluación:

Área: Redes y Conectividad.

Fecha:

Responsable: Milton Tarrillo Villegas

Apoyo:

Instrumentos:

- *Lista de Chequeo (en base a los requerimientos del Reglamento de la Ley 29733)*
- *Documento de Registro de Hallazgo.*
- *Reporte de entrevista*
- *ISO 17799, LPDP y RLPDP.*

2.5.2. Descripción de las desviaciones encontradas.

- ✓ Inexistentes documentos o cláusulas contractuales que limiten los detalles de la prestación de servicios internos.
- ✓ Inexistentes documentos o cláusulas contractuales que limiten los detalles de la prestación de servicios externos
- ✓ Inexistencia de compromisos de confidencialidad a los prestadores de servicios externos
- ✓ No garantizada destrucción de la información al terminar un servicio con terceros externos.

2.6. Dictamen

Luego de realizar la auditoria se obtuvieron los siguientes resultados de manera cuantitativa.

- **CONTROL : SEGURIDAD PARA EL TRATAMIENTO DE INFORMACIÓN DIGITAL**

a) Evaluar el control de accesos a la información

	VALOR	NO	PARCIAL	SI	TOTAL
1.1. Evaluar el control de acceso a la información	14.0%				0
1.1.1. ¿El Sistema Académico está protegido contra el acceso lógico no autorizado?	1.5%			x	1.5
1.1.2. ¿Se utilizan ID's únicos para dar acceso a los usuarios del Sistema Académico?	0.5%			x	0.5
1.1.3. ¿El servidor del sistema almacena contraseñas de inicio de sesión de manera cifrada?	1.0%			x	1
1.1.4. ¿Se permite que el usuario cambie la contraseña cuando lo desee?	0.5%			x	0.5
1.1.5. Para la creación de un nuevo usuario (Alumnos, Docentes, Administrativos)¿se revisa que el usuario tenga la autorización dada por el propietario del banco de datos?	1.0%		x		0.5
1.1.6. ¿Se requiere que las contraseñas contengan al menos 8 dígitos, números y al menos incluyan un carácter especial?	1.0%		x		0.5
1.1.7. Para la creación de un nuevo usuario (Alumnos, docentes, administrativos): ¿Revisa que el nivel otorgado sea apropiado para el propósito?	1.0%		x		0.5
1.1.8. Durante la creación de un nuevo usuario: ¿Se le proporciona a los usuarios un documento escrito de sus derechos de acceso?	1.0%	x			0
1.1.9. Para la creación de un nuevo usuario: ¿Se requiere a los usuarios la firma de un documento indicando el entendimiento de las condiciones de acceso?	1.0%	x			0
1.1.10. ¿DIGETI, se asegura que no se proporcione el acceso hasta haber completado los procedimientos de autorización?	1.0%			x	1
1.1.11. ¿Se mantiene un registro formal de todas las personas registradas para usar el servicio?	1.0%		x		0.5
1.1.12. ¿Se verifica la eliminación o bloqueo inmediato de los derechos de acceso a los usuarios que han cambiado de puesto o han dejado la organización?	1.5%			x	1.5
1.1.13. ¿Se asegura que no se emitan ID's redundantes a otros usuarios?	1.0%		x		0.5
1.1.14. ¿Se realiza un chequeo periódico para eliminar o bloquear los ID's de usuario o cuentas redundantes?	1.0%		x		0.5
TOTAL	14.0%				9.00

Resultado: Total 14 = 100 %
Alcanzado 9= 64.20%

b) Evaluar una correcta gestión de privilegios.

	VALOR	NO	PARCIAL	SI	TOTAL
1.2. Evaluar una correcta gestión de privilegios	8.0%				0
1.2.1. ¿Se cuentan con políticas donde se regule la disposición de privilegios al sistema?	1.0%	x			0
1.2.2. ¿Se tiene un proceso de autorización debidamente documentado?	1.0%	x			0
1.2.3. ¿Se otorga privilegios de acuerdo a la necesidad basándose las políticas de control de acceso?	1.0%	x			0
1.2.4. ¿Se mantiene un registro de todos los privilegios asignados a los usuarios?	1.0%			x	1
1.2.5. ¿Se verifica que no se otorguen privilegios hasta completar el proceso de autorización?	1.0%			x	1
1.2.6. ¿Los privilegios se asignan a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio?	1.0%	x			0
1.2.7. ¿Se revisan las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados?	1.0%		x		0.5
1.2.8. ¿Se revisan las autorizaciones para los usuarios con privilegios especiales en intervalos de tiempo más cortos?	1.0%		x		0.5
TOTAL					3

Resultados: Total: 8.0 = 100%
Alcanzado: 3 = 37.5%

c) Evaluar los reportes de accesos.

	VALOR	NO	PARCIAL	SI	TOTAL
1.3. Evaluar los reportes de accesos	4.0%				
1.3.1. ¿Se generan y mantienen registros que provean evidencia de accesos al sistema?	2.0%			x	2
1.3.2. ¿Hay trazabilidad en los registros de acceso al sistema, como: horas de inicio, cierre de sesión y acciones relevantes?	2.0%	x			0
TOTAL					**2.0**

Resultados: Total: 4.0 = 100%
Alcanzado: 2.0 = 50 %

d) Evaluar la realización del procedimiento documentado.

	VALOR	NO	PARCIAL	SI	TOTAL
1.4. Evaluar la realización del procedimiento documentado	4.0%				0
1.4.1. ¿Se cuenta con flujos de trabajos o procedimientos establecidos para el control de accesos?	1.5%	x			0
1.4.2. ¿Se realizan las actividades de acuerdo a los procedimientos documentados?	1.0%	x			0
1.4.3. ¿Se realizan auditorías de cumplimiento del control de accesos establecidos en la directiva de seguridad de la información de banco de datos	1.5%	x			0
					0.0

Resultados: Total: 4.0 = 100%
Alcanzado: 0.0 = 0 %

- **CONTROL: CONSERVACION, RESPLADO Y RECUPERACION DE DATOS PERSONALES.**

a) Evaluar el control de seguridad en los ambientes que contiene datos.

	VALOR	NO	PARCIAL	SI	TOTAL
2. Conservación, respaldo y recuperación de Datos Personales	25.0%				
2.1 Evaluar el control de seguridad en los ambientes que contienen datos	10.0%				
2.1.1 ¿Los perímetros del edificio o local que contienen los medios de almacenamiento de información son físicamente sólidos?	2.0%			x	2
2.1.2 ¿Las puertas y ventanas están protegidas de accesos no autorizados por mecanismos de control: Por ejemplo vallas, alarmas , relojes, etc.	2.0%			x	2
2.1.3 ¿Los medios de almacenamiento de información se encuentran físicamente separados de aquellos ajenos a la organización?	2.0%		x		1
2.1.4 ¿Se usan controles de autenticación para restringir el acceso a los ambientes de procesamiento y almacenamiento de Información personal?	2.0%		x		1
2.1.5 El personal de servicios de ajenos al área ¿cuenta con acceso restringido a las áreas seguras o los medios de procesamiento de Información Personal?	2.0%			x	2
TOTAL					**8.0**

Resultados: Total: 10.0 = 100%
Alcanzado: 8.0 = 80.0%

b) Evaluar los mecanismos de respaldo de la información.

	VALOR	NO	PARCIAL	SI	TOTAL
2.2 Evaluar los Mecanismos de respaldo de la información	8.0%				0
2.2.1 ¿Se mantienen copias de seguridad del banco de datos personales?	1.6%			x	1.6
2.2.2 ¿Las copias de respaldo de datos personales son protegidas mediante técnicas de cifrado?	1.6%	x			0
2.2.3 ¿Las copias de respaldo se almacenan en un lugar físicamente apartado del local principal, para evitar algún daño por algún accidente o desastre natural?	1.6%		x		0.8
2.2.4 La información de respaldo cuenta con el mismo nivel de seguridad física y ambiental que el local principal.	1.6%		x		0.8
2.2.5 ¿Los medios de respaldos se prueban regularmente para comprobar su correcto funcionamiento?	1.6%			x	1.6
TOTAL					**4.8**

Resultados: Total: 7.5 = 100%
Alcanzado: 4.8 = 64%

c) Evaluar los procedimientos de restauración de respaldo.

	VALOR	NO	PARCIAL	SI	TOTAL
2.3 Evaluar procedimientos de restauración de respaldos.	7.0%				0
2.3.1 ¿Los procedimientos de restauración se chequean y prueban regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación?	2.0%			x	2
2.3.2 ¿Las pruebas realizadas a los respaldos cuentan con la documentación adecuada?(fecha y hora de la prueba, nombre del que realizo, BDP recuperado, tiempo de recuperación, resultados de la pruebas)	1.0%	x			0
2.3.3 ¿Se toman acciones en caso de pruebas insatisfactorias?	2.0%			x	2
2.3.4 Cuando se restaura una copia de seguridad del banco de datos personales ¿se requiere autorización del titular de BDP o quien es te asignado?	2.0%			x	2
TOTAL					**6.0**

Resultados: Total: 7.5 = 100%
Alcanzado: 6 = 80%

- **CONTROL: TRANSFERECIA LOGICA O ELECTRONICA DE DATOS PERSONALES.**

a) Supervisar la autorización del titular del Banco de Datos Personales.

	VALOR	NO	PARCIAL	SI	TOTAL
3. Transferencia lógica o electrónica de Datos Personales.	30.0%				
3.1. Supervisar la autorización del titular del BDP para la transferencia.	10.0%				
3.1.1. Se cuentan con políticas para la transferencia lógica o electrónica de Datos Personales	2.5%		X		1.25
3.1.2. ¿El tratamiento de datos personales es autorizado por el titular del banco de datos personales?	2.5%			X	2.5
3.1.3. ¿Se cuenta con algún documento que garantice la trasferencia Internacional de Datos Personales?	2.5%	X			0
3.1.4. ¿Se procede a la transferencia Datos Personales aun sin la autorización previa del Titular de Banco de Datos o encargado?	2.5%			X	2.5
TOTAL					**6.3**

Resultados: Total: 10.0 = 100%
Alcanzado: 6.3 = %

b) Medios de transporte para transferencia de datos personales.

	VALOR	NO	PARCIAL	SI	TOTAL
3.2. Medios de transporte para la transferencia de datos personales.	10.0%				
3.2.1. ¿Se cuentan con medios de envío autorizados Titular de BDP para la trasferencia de Datos?	2.5%		X		1.25
3.2.2. ¿Se controle el uso de los medios de transferencia de datos personales?	2.5%		x		1.25
3.2.3. ¿Existe evidencia documentada del uso de los medios de transferencia establecidos?	2.5%	x			0
3.2.4. ¿Se utilizan software especializado para la transferencia de datos personales?	2.5%	x			0
TOTAL					**2.5**

Resultados: Total: 10.0 = 100%
Alcanzado: 2.5 = 25%

c) Mecanismos de seguridad en la transferencia de datos personales.

d)

	VALOR	NO	PARCIAL	SI	TOTAL
3.3. **Mecanismos de Seguridad en la transferencia de Datos Personales**	10.0%				
3.3.1. ¿Se encuentran establecidos los mecanismos de seguridad para la transferencia en las políticas?	2.0%			x	2
3.3.2. ¿Los equipos utilizados para la transferencia lógica cuentan con software de protección contra códigos maliciosos?	2.0%			x	2
3.3.3. ¿Se utilizan protocolos de comunicación cifrados como: VPN, correo electrónico cifrado, FTP seguro, otros?|	2.0%			x	2
3.3.4. Los datos contenidos en soporte informático ¿se transportan previa encriptación y un mecanismo de verificación de la integridad?	2.0%		x		1
3.3.5. El Área de tratamiento de datos personales tiene restringido el uso de herramientas de registro no autorizadas? (cámara de video , fotográficas, grabación de audio ,etc.)	2.0%	x			0
TOTAL					**7.0**

Resultados: Total: 10.0 = 100%
Alcanzado: 7.0 = 70%

- **CONTROL: PRESTACION DE SERVICIOS SIN ACCESO A DATOS PERSONALES.**

a) Servicios internos de la organización o área sin acceso a datos personales.

	VALOR	NO	PARCIAL	SI	TOTAL
4. Prestación de servicios sin acceso a datos personales	15.0%				
4.1. Servicios internos de la organización o área sin acceso a datos personales	10.0%				
4.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?	2.5%		x		1.25
4.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?	2.5%			x	2.5
4.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.	2.5%	x			0
4.1.4. ¿Se generan documentos mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?	2.5%	x			0
TOTAL					**3.8**

Resultados: Total: 15.00 = 100%

Alcanzado: 3.8 = 62.5%

b) Servicios externos a la organización a la organización sin accesos a datos personales.

	VALOR	NO	PARCIAL	SI	TOTAL
4.2. Servicios externos a la organización sin acceso a datos personales	5.0%				
4.2.1. ¿Se generan contratos expresos o cláusulas contractuales sobre el tratamiento de datos personales al momento de prestar servicios externos?	1.25%		x		0.625
4.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?	1.25%	x			0
4.2.3. ¿Existe algún documento que garantice la destrucción o imposibilidad de recuperación de los datos alojados en el servicio del prestador de servicio una vez concluida la relación con el proveedor?	1.25%		x		0.625
4.2.4. ¿Se realizan visitas a la infraestructura del proveedor para comprobar el cumplimiento del servicio? O en caso de un proveedor extranjero: ¿Los prestadores de servicio cuentan con reportes SOC para verificar el cumplimiento del servicio?	1.25%		x		0.625
TOTAL					**1.9**

Resultados: Total: 5.00 = 100%

Alcanzado: 1.9 = 37.5%

RESULTADOS FINALES

FACTORES PRIMARIOS	% TOTAL	% Alcanzado	Resultado Cualitativo
1. Seguridad para el tratamiento de la Información Digital	30 %	14 %	MEDIO
2. Conservación, respaldo y recuperación de los datos personales.	25 %	18.8 %	BUENO
3. Transferencia Lógica o Electrónica de los Datos Personales	30 %	15.75 %	MEDIO
4. Prestación de servicios sin acceso a datos personales	15 %	5.63 %	MALO
TOTAL	**100 %**	**54.2 %**	**MEDIO**

Como resultados finales se informa que de manera cuantitativa se evidencio un 54.2% de cumplimiento del total de la evaluación de las Medidas de Seguridad de la Ley N° 29733 en el Área de DIGETI; esto significa que solo se alcanzaron 54 puntos de los 100 contenidos en el instrumento utilizado, además se presenta que el factor en el que se tiene menos puntaje obtenido es en cuando la Prestación de Servicios sin acceso a datos personales, dentro de las recomendaciones se irán mostrando a detalle las recomendaciones para mejorar.

De la misma manera de manera cuantitativa se obtuvo un resultado de MEDIO, para el cumplimiento, lo que se espera que mejore luego de aplicar las recomendaciones.

3. PRESENTACIÓN DEL DICTAMEN (SECRETARIA GENERAL)

3.1. Breve introducción al dictamen

3.2. Área de auditoría: Secretaria General

3.2.1. Datos de Evaluación:

Área: Secretaria General

Fecha:

Responsable: Cristhian Calisaya Sana

Apoyo: Milton Tarrillo

Instrumentos:

- Lista de Chequeo (basados en los requerimientos del Reglamento de la Ley y la ISO en cuanto a medidas de Control de Acceso)
- Documento de Registro de Hallazgos
- ISO 17799:2007
- Cámara Fotográfica.

Duración de la entrevista: 70 min aprox.

3.2.2. Descripción de las desviaciones encontradas.

- ✓ Inapropiada separación de documentos que contienen datos personales para evitar su exposición.
- ✓ No garantizado proceso de autorización para generar o eliminar copias de documentos que contienen datos personales.
- ✓ Inexistente procedimiento de destrucción de documentos que garanticen la no recuperación.
- ✓ Inexistente documento que indique la responsabilidad ante algún incidente relacionado al acceso no autorizado a documentos que contienen datos personales.
- ✓ Deficiente procedimiento de autorización a los usuarios que deseen acceder a los documentos de datos personales.
- ✓ Inexistente documento de registro de los usuarios autorizados y no autorizados para el acceso al banco de datos.
- ✓ Inexistente documento de registro de personas que accedieron al banco de datos (Archivo Institucional).
- ✓ Inexistente documento de registro de los usuarios o mensajeros autorizados para trasladar la información con datos personales.
- ✓ Inexistente mecanismo de verificación de no vulneración del contenedor en el cual se trasporta la información.
- ✓ Inexistente registro de incidentes de seguridad relacionados a la gestión de los documentos que contienen datos personales.
- ✓ Inexistente procedimiento de comunicación al propietario de banco de datos luego de darse un incidente con datos personales.
- ✓ Deficiente control sobre el personal de la organización que presta otros servicios al área de Secretaria General.
- ✓ Deficiente control sobre el personal externo a la organización que presta servicios al área de Secretaria General.

3.3 Dictamen

- **Almacenamiento, copia y acceso a la documentación no automatizada.**

a) Almacenamiento de documentación automatizada

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
1. Almacenamiento, copia y acceso a la documentación no automatizada	**50.0%**				
1.1. Almacenamiento de documentación no automatizada	**20.0%**				
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.	8.0%			x	8
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?	6.0%			x	6
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?	6.0%		x		3
TOTAL	**20.0%**				**17**

Resultados:

Total: 20 = 100%

Alcanzado: 17 = 85%

b) Copia o reproducción de la documentación no automatizada

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
1.2. Copia o reproducción de la documentación no automatizada	**15.0%**				
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?	3.0%		x		1.5
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales sin permitir su recuperación.	3.0%	x			0
1.2.3. ¿Se utiiza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?	3.0%			x	3
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos	3.0%			x	3
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?	3.0%			x	3
TOTAL	**15.0%**				**10.5**

Resultados:

Total: 15 = 100%

Alcanzado: 10.5 = 70%

c) Acceso a la documentación no automatizada.

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
TOTAL	15.0%				10.5
1.3. Acceso a la documentación no automatizada	15%				
1.3.1 ¿Se cuenta con algún documento donde indique la responsabilidad que recae en el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos personales?	3.75%	x			0
1.3.2 ¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?	3.75%		x		1.875
1.3.3 ¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?	3.75%	x			0
1.3.4 ¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?	3.75%	x			0
TOTAL	15.0%				1.875

Resultados:

Total: 15 = 100%

Alcanzado: 1.88 = 12.5%

- **Traslado de la documentación no automatizada.**

  a) Medidas para impedir el acceso o manipulación a los datos personales de traslado.

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
2. Traslado de la documentación no automatizada	30%				
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado	17.5%				
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?	2.5%		x		2.5
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?	2.5%			x	2.5
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?	2.5%			x	1.25
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?	2.5%		x		2.5
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?	2.5%			x	0
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?	2.5%	x			1.25
2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.	2.5%		x		0
TOTAL	17.50%				10

Resultados:

Total: 17.5 = 100%

Alcanzado: 10 = 57.15

b) Eventos o incidentes en el traslado de datos personales.

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
2.2. Eventos o incidentes en el traslado de datos personales	**12.5%**				
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?	4.5%	x			0
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?	4.0%	x			2
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?	4.0%		x		0
TOTAL					**2**

Resultados:

Total: 12.5 = 100%

Alcanzado: 2 = 16 %

- **Prestación de servicios sin accesos a datos personales.**

a) Servicios Internos de la organización o área sin acceso a datos personales

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
3.1. Servicios internos de la organización o área sin acceso a datos personales	**10%**				
3.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?	2.5%	x			0
3.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?	2.5%	x			2.5
3.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.	2.5%			x	0
3.1.4. ¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?	2.5%	x			0
TOTAL	**10%**				**2.5**

Resultados:

Total: 10 = 100%

Alcanzado: 2.5 = 25 %

b) Servicios externos a la organización sin accesos a datos personales.

Actividades a evaluar		NO	PARCIAL	SI	TOTAL
3.2. Servicios externos a la organización sin acceso a datos personales	**10%**				0
3.2.1. ¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?	3.5%	x			0
3.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?	3.5%	x			0
3.2.3. ¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?	3.0%	x			0
TOTAL	**10%**				**0**

Resultados:

Total: 10 = 100%

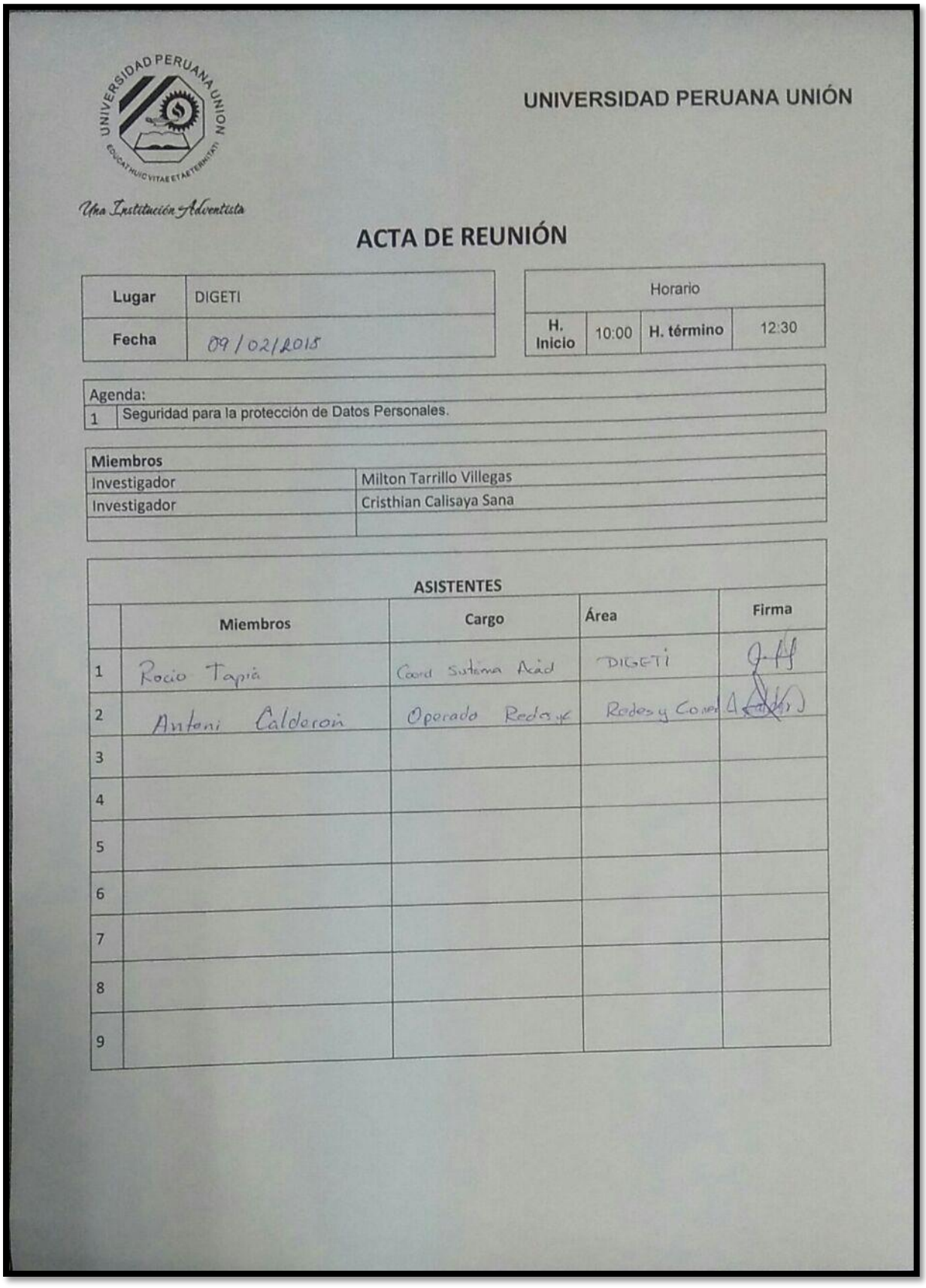
Alcanzado: 0 = 0 %

Resultados Finales

FACTORES PRIMARIOS	% TOTAL	% Alcanzado	Resultado Cualitativo
1. Almacenamiento, copia y acceso a la documentación no automatizada.	50 %	29 .38%	MEDIO
2. Traslado de la documentación no automatizada.	30 %	12%	MEDIO
3. Prestación de servicio sin acceso a datos personales.	20 %	2.5 %	BAJO
TOTAL	**100 %**	**43.88 %**	**MEDIO**

Como resultados finales de la evaluación a Secretaria General se obtuvo las siguientes cifras: De manera cuantitativa se obtuvieron un 43 % de los puntos de la evaluación, menos de la mitad del total de los requerimientos en medidas de seguridad fueron demostrados; de manera cualitativa obtuvo un nivel: MEDIO, además que se evidencio bajos niveles en el factor N°3: "Prestación de Servicios sin acceso a datos personales"; se espera que luego de esta evaluación y con las propuestas a presentarse el nivel y porcentaje de cumplimiento suba ya que la causa principal de las no conformidades es que no se cuentan con las medidas por desconocimiento del tema.

Anexo 7. Acta de reunión del personal de DIGETI



UNIVERSIDAD PERUANA UNIÓN

Una Institución Adventista

ACTA DE REUNIÓN

Lugar	DIGETI
Fecha	09/02/2015

Horario			
H. Inicio	10:00	**H. término**	12:30

Agenda:	
1	Seguridad para la protección de Datos Personales.

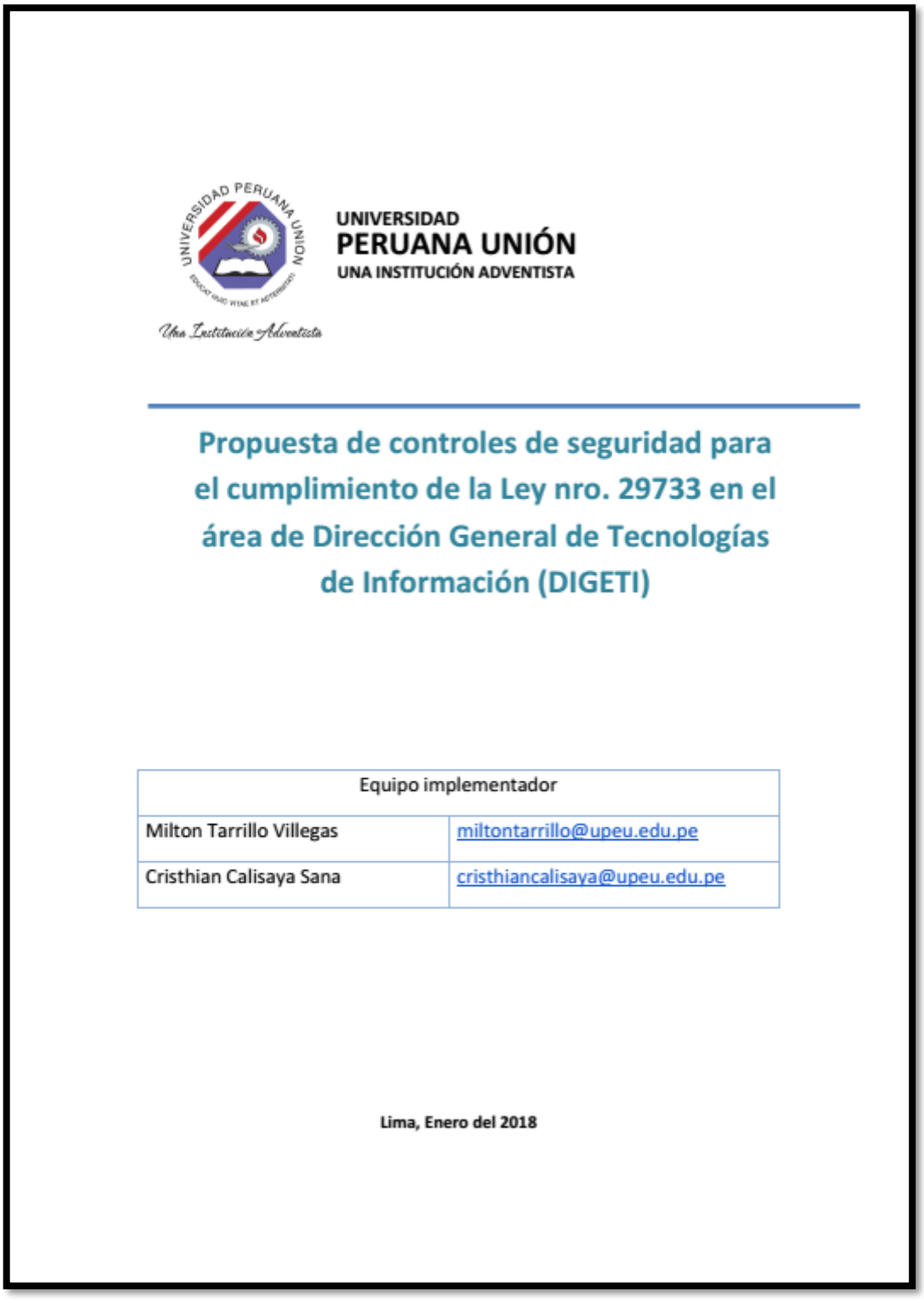
Miembros	
Investigador	Milton Tarrillo Villegas
Investigador	Cristhian Calisaya Sana

ASISTENTES

	Miembros	Cargo	Área	Firma
1	Rocio Tapia	Coord Sistema Acad	DIGETI	
2	Antoni Calderon	Operado Redes	Redes y Com	
3				
4				
5				
6				
7				
8				
9				

Anexo 8. Registro fotográfico con el personal de DIGETI

Anexo 9. Propuesta de controles para DIGETI



UNIVERSIDAD
PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

Una Institución Adventista

Propuesta de controles de seguridad para el cumplimiento de la Ley nro. 29733 en el área de Dirección General de Tecnologías de Información (DIGETI)

Equipo implementador	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Lima, Enero del 2018

INDICE

I. GLOSARIO

Información: Es la interpretación que se le da a un conjunto de datos, puede estar de manera física como lógica.

Datos personales: Es aquella información que hace identificable a toda persona natural como: nombres, dirección, sexo, edad, etc.

Controles/Control: Es un mecanismo utilizado para asegurar un determinado servicio y/o activo. Los controles pueden ser procedimientos, formatos, tecnología, etc.

Política: Es una guía orientada a la acción que debe ser divulgada, entendida y acatada por los miembros de una organización o área (siendo el caso de la investigación).

Política general: Es una guía a nivel de aplicación general, su impacto es alto y crítico.

Política específica: Es una guía con un nivel menor, determina ciertos procesos y es delimitado por su alcance.

Seguridad lógica: Es la aplicación de medidas para la protección de información entre amenazas de manera digital.

Banco de datos lógico: Es un conjunto de datos personales en soporte automatizado

Tratamiento de datos personales: Es cualquier operación que permite la recolección, conservación, modificación o eliminación de datos personales.

Trazabilidad: Es la capacidad de registro de las operaciones y/o actividades realizadas desde su origen hasta su destino.

Procedimiento: Es un modelo de conjunto de acciones que debe realizarse para lograr un objetivo.

Confidencialidad: Es el aseguramiento del acceso a documentos solo por personas autorizadas.

Integridad: Es el aseguramiento de información exacta, verídica y completa.

Disponibilidad: Es el aseguramiento de la información y/o servicio a las personas que lo requieran en todo momento.

Respaldo: Es la acción de realizar una copia a la información independientemente del tipo de respaldo que se realice (normal o total)

Recuperación: Es la acción de poner en disponibilidad al respaldo realizado con anterioridad.

II. INTRODUCCIÓN

La información se puede encontrar de forma digital o física, sin embargo, cual sea el caso, es necesario adoptar medidas para asegurar su confidencialidad, integridad y disponibilidad.

El área de DIGETI es el encargado de velar por la seguridad, controlar y mantener en funcionamiento las TICS (Tecnologías de información y la comunicación) dentro de la Universidad Peruana Unión (UPeU). El trabajo en conjunto con las sub áreas implica el tratamiento de datos personales, desde la creación de un usuario, los controles de acceso a la información, hasta la transferencia y respaldo de la misma.

Por lo tanto, para asegurar un mejor servicio y proteger la información de manera óptima será necesario implantar controles que se adecuen al entorno organizacional, estas pueden ser: políticas, prácticas, procedimientos, estructuras organizativas, funciones de software y hardware, etc.

De la misma forma para el cumplimiento de la Ley nro. 29733 (Ley de Protección de datos personales) en su apartado "Medidas de Seguridad" el presente documento propondrá controles de seguridad basados en la NTP-ISO/IEC 17799:2007, la cual ofrece recomendaciones para realizar una adecuada gestión de la seguridad de la información.

III. CUMPLIMIENTO DE LA METODOLOGÍA

Considerando el término de la primera y segunda etapa de la metodología que se muestra en la Figura 1;

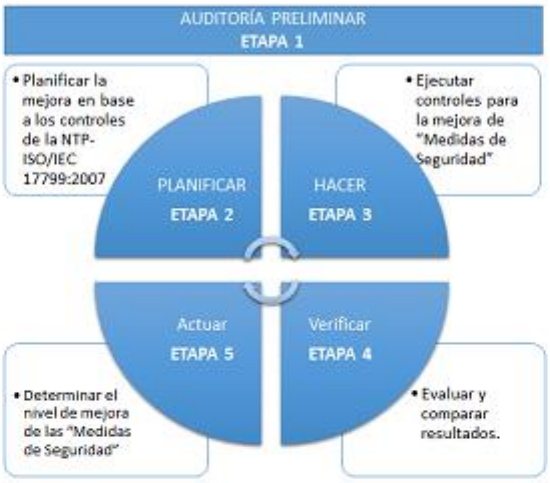


Figura1. Etapas de la metodología

Se procede a realizar las actividades pertenecientes a la tercera etapa *Ejecutar controles* que se contempla en la Figura 2.

Figura 2. Actividades para la ejecución de controles

IV. PROPUESTA DE CONTROLES DE SEGURIDAD

Basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007, la propuesta está estructurada en dos partes.

A. Control de seguridad general

La siguiente política general, refleja los controles específicos del presente documento. La política está desarrollada en base a la necesidad del área y la organización, por lo que se propone lo siguiente:

1. Política de seguridad digital para la protección de datos

Código de propuesta: PD001	**Tipo**: Documento
Clausula: POLÍTICA DE SEGURIDAD	
Control: Documento de política de seguridad de la información.	
Alcance: La política general es aplicable a todo el personal de DIGETI y trabajadores de la UPeU que realicen labores directamente con el área, también, a los usuarios externos que presten o prestare servicios al área. Implicará las actividades relacionados al (o la): 1. Seguridad para el tratamiento información digital 2. Conservación, respaldo y recuperación de datos personales 3. Transferencia lógica o electrónica de datos personales 4. Prestación de servicios sin acceso a datos personales	
Solución: Implementar una política de seguridad para la protección del banco de datos automatizado en DIGETI, para dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos del negocio, leyes y regulaciones. La política reflejará en absoluto los controles propuestos de la investigación.	
Documento adjunto: Ver el Anexo 01 para la política general.	

B. Control de seguridad específico

La propuesta de los siguientes controles se elaboró en base a los hallazgos encontrados en la evaluación previa y las cuales están reflejadas en la política general.

1. Seguridad para el tratamiento de la Información Digital

1.1. Evaluar el control de acceso a la información

1.1.1. Nombre de la propuesta: Proceso para la Gestión de usuarios y privilegios

<table>
<tr><td>Código de hallazgo: RD001, RD002, RD003, RD006, RD007, RD008, RD009, RD010, RD011, RD012, RD013, RD014</td><td>Código de propuesta: PD002</td></tr>
<tr><td colspan="2">Descripción del hallazgo: El personal de DIGETI realiza sus actividades empíricamente, mas no se tiene un proceso documentado que refleje las actividades, tareas y otros aspectos para medir el proceso de creación de usuarios y privilegios. Así mismo, no se tiene un cronograma con fechas definidas para la revisión de accesos y privilegios.</td></tr>
<tr><td colspan="2">Clausula: CONTROL DE ACCESOS</td></tr>
<tr><td>Control: Política de control de accesos, Gestión de accesos de usuario, Gestión de contraseñas de usuario</td><td>Tipo: Proceso y Política</td></tr>
<tr><td colspan="2">Alcance: El área de Desarrollo de Sistemas y Mesa de Ayuda trabajarán en conjunto para él y cumplimiento del Proceso de Gestión de Usuarios, su alcance será el uso de contraseñas para el Sistema Académico.</td></tr>
<tr><td colspan="2">Solución:
El sub área de Mesa de Ayuda y Desarrollo de Sistemas trabajarán en conjunto para el desarrollo y cumplimiento de la política, considerando a las áreas y/o alumnos de la universidad que soliciten del servicio. La política y el documento abarcarán únicamente el Sistema Académico. Incluye:

✓ Implementar un procedimiento formal para estandarizar una correcta autorización de privilegios al Sistema Académico, identificando los pasos que se debe seguir para ejecutar las solicitudes (Anexo 02); y realizar periódicamente revisión de los accesos y privilegios otorgados (Anexo 02).
✓ Directriz de contraseñas seguras (Anexo 03)</td></tr>
<tr><td colspan="2">Documento adjunto: Ver el Anexo 02 para el procedimiento de Gestión de usuarios y privilegios, el anexo 03 para la Directriz.</td></tr>
</table>

1.1.2. Nombre de la propuesta: Formato de derechos de acceso

Código de hallazgo: RD004, RD005	**Código de propuesta**: PD003
Descripción del hallazgo: El sub área de Mesa de Ayuda realiza la creación de los usuarios al portal sea presencial o no, pero no indica al usuario que accesos se le está otorgando y obtener su entendimiento.	
Clausula: CONTROL DE ACCESOS	
Control: Política de control de accesos, Registro de usuarios	**Tipo**: Formato
Alcance: Su alcance es sólo en la creación de usuarios para el portal académico. Incluirá el formato físico o mensaje por correo electrónico según sea el caso.	
Solución: Se implementará un formato de los derechos de acceso que tendrá el usuario y una firma manifestando su entendimiento.	
Documento adjunto: Ver el Anexo 04 para el formato de derechos de acceso.	

1.2. Evaluar una correcta gestión de privilegios

Para los hallazgos con código: **RD009, RD010, RD011, RD012, RD013, RD014** que está relacionado con gestión de privilegios, se sugiere la propuesta Proceso para la Gestión de usuarios y privilegios con código: **PD002.**

1.3. Evaluar los reportes de accesos

Respecto al hallazgo con código **RD015**, esta actividad cumple parcialmente con los predichos de la NTP-ISO/IEC 17799:2007; sin embargo, por la coyuntura organizacional del Proyecto ERP se sugiere considerar el documento de Recomendaciones del Anexo 15.

1.4. Evaluar la realización del procedimiento documentado

Para los hallazgos con código: **RD016 y RD017** que está relacionado con el cumplimiento de un procedimiento establecido para el control de accesos, se sugiere la propuesta proceso para la Gestión de usuarios y privilegios con código: **PD002.**

1.4.1. Nombre de la propuesta: Cronograma de auditoría en el control de accesos

Código de hallazgo: RD018	**Código de propuesta**: PD004
Descripción del hallazgo: Ausencia de realización de auditorías para verificar el cumplimiento del proceso de control de accesos	
Clausula: CUMPLIMIENTO	
Control: Registro de la auditoría	**Tipo**: Cronograma (registro)
Alcance: Su alcance es sobre el cumplimiento del proceso de Gestión de usuarios y privilegios	
Solución: Desarrollar un programa anual que refleje las fechas específicas, y el responsable para realizar una evaluación de cumplimiento del proceso de control de accesos.	
Documento adjunto: Ver el Anexo 05 para el Programa anual de auditorías y el anexo 06 para Plan de auditorías internas.	

Para el hallazgo con código: **RD018** que está relacionado con la evaluación del cumplimiento del control de accesos, se sugiere la propuesta del proceso para la Gestión de usuarios y privilegios con código: **PD002**.

2. Conservación, respaldo y recuperación de datos personales

2.1. Evaluar el control de seguridad en los ambientes que contienen datos

2.1.1. Nombre de la propuesta: Política para el respaldo y recuperación

Código de hallazgo: RD019, RD022, RD023, RD024	**Código de propuesta**: PD005
Descripción del hallazgo: DIGETI realiza back ups continuamente pero no se realiza un registro de cada acción realizada. También, mantiene una copia de otra organización perteneciente a la red, pero sin ningún contrato por medio. Así mismo, mantiene una réplica dentro de una zona geográfica no permitida.	
Clausula: GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Control: Gestión de respaldo y recuperación	**Tipo**: Política específica y Formato
Alcance: El alcance de la política es sobre las labores que realiza el sub área de Redes y Conectividad sobre el "Centro de datos" y, los mismos que serán los responsables de velar por el cumplimiento de la política y el formato.	
Solución: Implementar una **política** específica y un **formato** que contemple las medidas y requisitos que se deberán tomar los encargados de DIGETI al realizar respaldos y la recuperación de la misma.	
Documento adjunto: Ver el Anexo 07 para la política y el anexo 08 para el formato de control de back ups.	

2.1.2. Nombre de la propuesta: Aseguramiento de autentificación al Centro de Datos

Código de Hallazgo: RD020	**Código de Propuesta**: PD006
Descripción del hallazgo: Existe un control de seguridad en el centro de datos, pero actualmente tiene algunas deficiencias con el carnet, puerta y alarma.	
Clausula: SEGURIDAD FISICA Y DEL ENTORNO	
Control: Perímetro de seguridad física y Controles físicos de entradas	**Tipo**: Tecnología
Alcance: El aseguramiento de autentificación se realizará en el Centro de Datos de DIGETI. El encargado de la implementación será una empresa tercera pero el responsable o responsables de controlar los accesos serán los trabajadores del sub área de Redes y Conectividad según la política de control físico.	
Solución: Mejorar el control de autentificación para autorizar y validar el acceso (visitas) al Centro de Datos. Renovar las alarmas, rejas u otros controles de acceso físico al Centro de Datos.	
Documento adjunto: Las Recomendaciones tecnológicas para este hallazgo se encuentra en el Anexo 15, así mismo para controlar el acceso al centro de datos ver el Anexo 09.	

2.2. Evaluar los mecanismos de respaldo de la información

Para el hallazgo con código: **RD021** que está relacionado con la ausencia de técnicas de cifrado para proteger las copias de respaldo de los datos personales se sugiere las Recomendaciones del Anexo 15.

2.3. Evaluar procedimientos de restauración de respaldos

Para el hallazgo con código: **RD024**, que está relacionado con la ausencia de una documentación adecuada de los respaldos, se sugiere la propuesta de solución Política para el respaldo y recuperación, con código: **PD005.**

3. Transferencia lógica o electrónica de datos personales

3.1. Supervisar la autorización del titular del banco de dato personal (BDP) para la transferencia

3.1.1. Nombre de la propuesta: Política de transferencia lógica de datos

Código de hallazgo: RD025, RD026, RD027, RD028, RD029, RD030	**Código de propuesta**: PD007
Descripción del hallazgo: Actualmente DIGETI tiene deficiencias al momento de autorizar la transferencia de datos por el encargado del banco de datos. Así mismo al momento de garantizar y evidenciar la confidencialidad e integridad en la transferencia lógica de datos con alguna organización externa.	
Clausula: GESTIÓN DE COMUNICACIONES Y OPERACIONES Y ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
Control: Intercambio de información, Servicios de correo electrónico y Política de uso de los controles criptográficos	**Tipo**: Política especifica
Alcance: La política será aplicable a las sub áreas de Desarrollo Académico y Redes y conectividad bajo su responsabilidad. El Director de DIGETI como Encargado del Banco de Datos evaluará y autorizará la transferencia (nacional e internacional).	
Solución: Implementar una **política** especifica que señale la obligación y necesidad de obtener la autorización para las transferencias, los mecanismos adecuados para garantizar la seguridad durante la transferencia (nacional e internacional), así mismo reflejará la necesidad de registrar la transferencia exitosa y el uso de los medios de transferencia permitidos. Desarrollar formato modelo para la autorización de transferencias.	
Documento adjunto: Ver el Anexo 10 para la política, el Anexo 11 para el formato para la autorización de transferencia de datos.	

3.2. Medios de transporte para la transferencia de datos personales

3.2.1. Para el hallazgo con código: **RD028, RD029, RD030**, que está relacionado con la ausencia de medios de transportes autorizados por el Titular del Banco de Datos y su evidencia documentada, se sugiere la propuesta con código: **PD007.**

3.2.2. Para el hallazgo con código: **RD031**, que está relacionado con el uso de un software especializado para la transferencia de datos personales, ver el Anexo 15 de Recomendaciones.

3.3. Mecanismos de seguridad en la transferencia de datos personales

3.3.1. Para el hallazgo con código: **RD032**, que está relacionado con la ausencia de algún soporte informático que permita enviar datos encriptados, ver el Anexo 15 de Recomendaciones.

4. Prestación de servicios sin acceso a datos personales

4.1. Servicios internos de la organización o área sin acceso a datos personales

4.1.1. Nombre de la propuesta: Política específica de control físico

Código de hallazgo: RD033, RD034	**Código de propuesta**: PD008
Descripción del hallazgo: Actualmente en DIGETI no existe un documento que límite la realización de trabajos y el acceso de personal interno (UPeU) al área o externo sea otra organización respecto al centro de datos.	
Clausula: SEGURIDAD FÍSICA Y DEL ENTORNO, ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Controles físicos de entradas, Seguridad en los accesos de terceras partes	**Tipo**: Política
Alcance: La política será al nivel de área (política específica). El personal de DIGETI, externos a la organización y demás áreas de la UPeU que deseen acceder al área de datos deberán cumplir la política.	
Solución: Implementar una política específica donde señale detalladamente quienes son las personas autorizadas al área de datos. Se supervisará y monitoreará las visitas al Área de Datos. El documento cumplirá con lo siguiente: • Limitar el acceso del personal ajeno al área a documentos que contengan datos personales. • Limitar la realización de trabajos que no impliquen el tratamiento de datos personales. • Restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de datos, salvo autorización del titular del banco de datos personales o encargado.	
Documento adjunto: Ver el Anexo 12 para la política de control de acceso físico.	

4.2. Servicios externos a la organización sin acceso a datos personales

4.2.1. Nombre de la propuesta: Instrucción para la gestión de acuerdos

Código de hallazgo: RD035, RD036, RD037, RD038, RD039	**Código de propuesta**: PD009
Descripción del hallazgo: Actualmente no se gestiona la seguridad en la contratación de servicios externos. Teniendo en cuenta la labor que realizaran por medio de cláusulas contractuales o documentos que respalden su seguridad.	
Clausula: GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Control: Gestión de servicios externos	**Tipo**: Política
Alcance: La Dirección de DIGETI y el personal encargado de gestionar los servicios deberá considerar la instrucción al momento de contratar algún servicio externo donde traten de datos personales.	
Solución: Implementar una instrucción para una correcta gestión de servicios (contractuales y/o legales) donde los terceros que presten servicios a la UPeU por encargo de DIGETI, estén enterados de sus obligaciones y responsabilidades que implique acceder, procesar, comunicar o manejar la información de la organización.	
Documento adjunto: Ver el Anexo 13 para el instructivo de gestión de acuerdos	

4.2.2. Nombre de la propuesta: Acuerdo de confidencialidad

Código de hallazgo: RD037	**Código de propuesta**: PD010
Descripción de hallazgo: El personal interno de DIGETI no cuenta con un documento donde describa la confidencialidad que deberá guardar durante la prestación de sus servicios. El personal realiza sus labores sin declarar el compromiso que tendrá al tratar con información sensible.	
Clausula: ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Acuerdos de confidencialidad	**Tipo**: Documento
Alcance: El documento de acuerdo de confidencialidad será firmado por el personal de DIGETI, otorgando de esa manera la comprensión del acuerdo y su compromiso.	
Solución: Implementar un documento contractual para los empleados de DIGETI donde acepten y firmen los términos y condiciones del contrato del empleo. El documento también considerará las responsabilidades, derechos y las acciones que se ha de tomar en caso incumpla el acuerdo durante el periodo de tiempo definido.	
Documento adjunto: Ver el Anexo 14 para el acuerdo de confidencialidad.	

ANEXOS

ANEXO 01

POLÍTICA DE SEGURIDAD PARA LA PROTECCIÓN DEL BANCO DE DATOS AUTOMATIZADO

POLITICA DE SEGURIDAD PARA LA PROTECCION DEL BANCO DE DATOS AUTOMATIZADO

Una Institución Adventista

UNIVERSIDAD PERUANA UNIÓN

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN (DIGETI)

Importante: DIGETI se reserva el derecho de modificar la presente política para adaptarla a cambios administrativos o legislativos.

INFORMACIÓN DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
----------	----------	----------
Equipo Investigador	Director de Dirección General de Tecnologías de Información	Director de Dirección General de Tecnologías de Información

CONTROL DE VERSIONES				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)	01/2018	Elaboración inicial	Todas	Equipo Inv.
1				
2				
3				

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El área de Dirección General de Tecnologías de Información (DIGETI) es un órgano[1] de apoyo y de soporte tecnológico en las actividades académicas, y de las áreas financieras contables de la Universidad Peruana Unión (UPeU).

Dentro de sus unidades (o sub áreas), la DIGETI está constituida por: Redes y Conectividad, Desarrollo de Sistemas, Mesa de Ayuda, Coordinación de Servicios Computacionales y la Dirección General.

DIGETI entiende la importancia de proteger la información, reconociendo a este como un activo importante para la organización y también la obligación de cumplir con la Ley de Protección de Datos Personales (LPDP) a nivel organizacional. Que en efecto disminuirá los incidentes relacionados a la seguridad de la información, ofreciendo un mejor servicio en función de nuestras facultades como DIGETI de acuerdo al estatuto de la UPeU.

Por ello, se establece la presente política de seguridad lógica para regular y asegurar el manejo de la información durante el proceso de su tratamiento en el área (seguridad en el tratamiento; conservación, respaldo y recuperación; transferencia lógica y prestación de servicios) de los datos personales.

Esta política general está constituida en base a los lineamientos de seguridad descritos por la NTP-ISO/IEC 17799:2007, de acuerdo a la necesidad del negocio de la organización y los requerimientos de la LPDP.

1. Estatuto, Resolución Nº002-2017/UPeU-AU

2. OBJETIVOS

La política de seguridad lógica para la protección de datos personales tiene los siguientes objetivos:

- Proteger la información de la organización soportada por los sistemas informáticos, conservando los atributos de confidencialidad, integridad y disponibilidad.
- Reforzar el control de respaldos y su recuperación; el acceso al data center y equipos informáticos que almacenen datos personales.
- Disminuir incidentes y la materialización de riesgos relacionados a la vulneración de la privacidad
- Gestionar las actividades de proveedores de servicios para mantener un nivel de seguridad óptimo.
- Promover una cultura de seguridad de la información.
- Cumplir con la Ley de Protección de Datos Personales en la UPeU.

3. ALCANCE

Esta política se aplica a todo el personal de DIGETI, el personal de la UPeU que realice labores directamente con el área, y también a usuarios externos que presten o prestaren servicios al área. Así mismo, implica las actividades relacionadas a la:

- Seguridad para el tratamiento de la información digital
- Conservación, respaldo y recuperación de datos personales
- Transferencia lógica o electrónica de datos personales
- Prestación de servicios sin acceso a datos personales

Enfatizando el acceso al Área de Datos (Centro de Datos), la cual contiene información fidedigna y critica para la UPeU.
La política abarca el cumplimiento de la Ley de Protección de Datos Personales para el capítulo IV "Medidas de Seguridad", en específico lo relacionado a la seguridad lógica, considerando los controles de seguridad de acuerdo a la necesidad del área y la organización, recomendados por la NTP-ISO/IEC 17799:2007, un documento que ofrece una adecuada gestión de la seguridad de la información. Las clausulas son las siguientes:

- Control de accesos
- Cumplimiento
- Gestión de comunicación y operaciones
- Seguridad física y del entorno
- Aspectos organizativos para la seguridad

4. DEFICINICIONES Y TÉRMINOS

Información: Es la interpretación que se le da a un conjunto de datos, puede estar de manera física como lógica.

Datos personales: Es aquella información que hace identificable a toda persona natural como: nombres, dirección, sexo, edad, etc.

Controles/Control: Es un mecanismo utilizado para asegurar un determinado servicio y/o activo. Los controles pueden ser procedimientos, formatos, tecnología, etc.

Política: Es una guía orientada a la acción que debe ser divulgada, entendida y acatada por los miembros de una organización o área (siendo el caso de la investigación).

Política general: Es una guía a nivel de aplicación general, su impacto es alto y crítico.

Política específica: Es una guía con un nivel menor, determina ciertos procesos y es delimitado por su alcance.

Banco de datos lógico: Es un conjunto de datos personales en soporte automatizado

Tratamiento de datos personales: Es cualquier operación que permite la recolección, conservación, modificación o eliminación de datos personales.

Procedimiento: Es un modelo de conjunto de acciones que debe realizarse para lograr un objetivo.

Confidencialidad: Es el aseguramiento del acceso a documentos solo por personas autorizadas.

Integridad: Es el aseguramiento de información exacta, verídica y completa.

Disponibilidad: Es el aseguramiento de la información y/o servicio a las personas que lo requieran en todo momento.

Respaldo: Es la acción de realizar una copia a la información independientemente del tipo de respaldo que se realice (normal o total)

Recuperación: Es la acción de poner en disponibilidad al respaldo realizado con anterioridad.

Anexo 03

DIRECTRIZ DE CONTRASEÑAS SEGURAS

Directriz de contraseñas seguras		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: DSD009

Directriz de contraseñas seguras

Las sub áreas de Desarrollo de Sistemas y Mesa de Ayuda son los responsables de desarrollar y mantener el proceso de creación/modificación de un nuevo usuario respetando el Proceso de Gestión de Usuarios y Privilegios (**PRD-01**). Durante el desarrollo del proceso se mantendrá la confidencialidad de las contraseñas; se le comunicará al usuario evitar **guardar registros de papel**, se prohibirá que el sistema permita contraseñas vulnerables a ataques de diccionario y tengan caracteres consecutivos o repetitivos. Las contraseñas cumplirán con al menos:

-Ocho (8) digitos,

-Ser alfanuméricos y,

-En lo mínimo tendrá un carácter especial.

Al crear la cuenta de usuario a una persona, se le enviará un mensaje al correo electrónico previamente otorgado por la persona, donde se le facilitará la contraseña por defecto a cambiar con urgencia (cuando ingrese por primera vez le pedirá el cambio de contraseña).

Así mismo no se deberá mostrar la contraseña en la pantalla al introducirla. Las contraseñas se guardarán en forma cifrada.

DIGETI se reserva el derecho de modificar el presente documento para adaptarlo a cambios administrativos o legislativos.

5. RESPONSABILIDADES Y CUMPLIMIENTO

5.1. RESPONSABILIDADES

Responsable del Banco de Datos Lógico: Director de DIGETI

Encargado del Banco de Datos Lógico: Jefe de Redes y Conectividad

Responsable de la Transferencia de Datos Personales: Jefe de Desarrollo de Sistemas

Encargado del proceso de Gestión de Usuarios: Jefe de Desarrollo de Sistemas y Jefe de Mesa de Ayuda

Asesor y/o Consultor: Secretario General

5.2. CUMPLIMIENTO

La presente política, entra en vigencia una vez aprobado por el Director de DIGETI.

El trabajador que ingrese al área con posterioridad a la fecha de aprobación, se le entregará una copia del presente documento y así mismo deberá declarar su conocimiento y aceptación con una firma.

La política está alineada a las necesidades propias del área y la organización, como también a la legislación existente (Ley 29733), cualquier cambio administrativo, organizacional o respecto a la normatividad se deberá informar inmediatamente al responsable del documento.

6. POLÍTICA

6.1. SEGURIDAD PARA EL TRATAMIENTO DE LA INFORMACIÓN DIGITAL

- Toda creación de usuarios o asignación de privilegios se realizará cumpliendo el procedimiento de Gestión de Usuarios y Privilegios (PRD-01), y finalizando con una firma en el documento de Derechos de acceso como parte de su entendimiento (DSD001).
- Los responsables del desarrollo de sistemas y los operadores de Mesa de Ayuda deberán trabajar en base a la Directriz de contraseñas seguras (DSD009).
- Las auditorías serán estipuladas en el documento Programa anual de auditoría (DSD002) y su ejecución será en base al Plan de Auditorías Internas (DSD003).

6.2. CONSERVACIÓN, RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

- Las actividades de almacenamiento, respaldo y recuperación serán realizadas en base a la Política específica de Almacenamiento y Respaldo (PSD002)
- Todo respaldo de la información será debidamente documentado en el formato de Control de Backups (DSD005).
- Todo acceso de terceros al Data Center deberá ser registrado en el documento Resumen de visitas al Data Center (DSD004), así mismo se cumplirá la Política específica para el acceso físico (PSD004)

6.3. TRANSFERENCIA LÓGICA O ELECTRÓNICA DE DATOS PERSONALES

- Toda transferencia lógica de datos personales se realizará respetando la Política específica para la Transferencia de Datos (PSD003)
- Toda transferencia lógica de datos personales será autorizada por el Director de DIGETI. Si el medio fuese email se utilizará el formato para la autorización de traslado (DSD006); o, se presentará un documento formal según la Política de Transferencia de Datos.

6.4. PRESTACIÓN DE SERVICIOS SIN ACCESO A DATOS PERSONALES

- Todo trabajo que implique el acceso de terceros al Data Center deberá cumplir con la Política específica para el acceso físico (PSD004)
- Toda contratación de servicios que implique tratamiento de datos personales se deberá realizar según las especificaciones del Instructivo para la gestión de acuerdos (DSD008).
- Todo el personal de DIGETI deberá declarar su entendimiento y aceptación mediante una firma sobre el Compromiso de confidencialidad (DSD007).

ANEXO 02

PROCEDIMIENTO DE GESTIÓN DE USUARIOS Y PRIVILEGIOS

UNIVERSIDAD PERUANA UNIÓN

Una Institución Adventista

Procedimiento
Gestión de Usuarios y Privilegios

N° de procedimiento:	PRD-01	
Versión actual	Nº1, 07 de Enero del 2018	
Versión anterior		
Aprobado por Dueño del proceso	**Revisión apoyo metodológico**	**Revisado por**
Director DIGETI	Equipo Investigador Gestión de Procesos	Immer Elias Cuellar Rodríguez

Contenido

Modelos Visuales

Flujograma de información con sus listas de tareas

a) Tipo Usuario: Docente

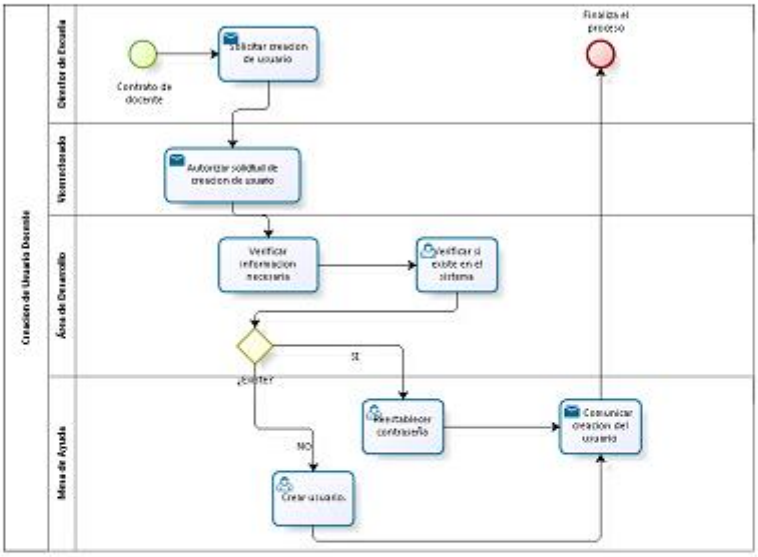


Fig.1 - Proceso de Creación de Usuario: Docente

Lista de Tareas			
Director de Escuela	**Vicerrectorado**	**Área de Desarrollo de Sistemas**	**Mesa de Ayuda**
Solicitar Creación de usuario ▪ Enviar un correo solicitando la creación de usuario con los datos del nuevo docente.	**Autorizar solicitud de creación de usuario** - Autoriza la solicitud teniendo en cuenta los requisitos: tener grado de Magister o tener experiencia docente antes del 2014.	**Verificar información necesaria:** ▪ Se verifican que la información personal recibida sea la necesaria para realizar la creación de usuario **Verificar si existe en el sistema** ▪ Se revisa si el nombre del docente ya está registrado o es nuevo.	*Si la condición es SI:* **Se reestablece la contraseña** Se reestablece la contraseña a una genérica para que pueda ingresar el docente. *Si la condición es NO:* **Crear Usuario** Se crea el usuario en el sistema académico

			Comunicar la creación del usuario: - Se envía un correo con el usuario creado y su contraseña genérica respectiva.

Información General

Evento activador	El proceso se activa cuando un nuevo docente es contratado para la Escuela Profesional
Objetivo	Establecer un procedimiento documentado, que informe y ayude en la gestión de las actividades de la creación de usuarios para docentes nuevos
Dueño	Área de Desarrollo Sistemas
Cliente	Dirección de Escuela

b) Tipo Usuario: Alumno

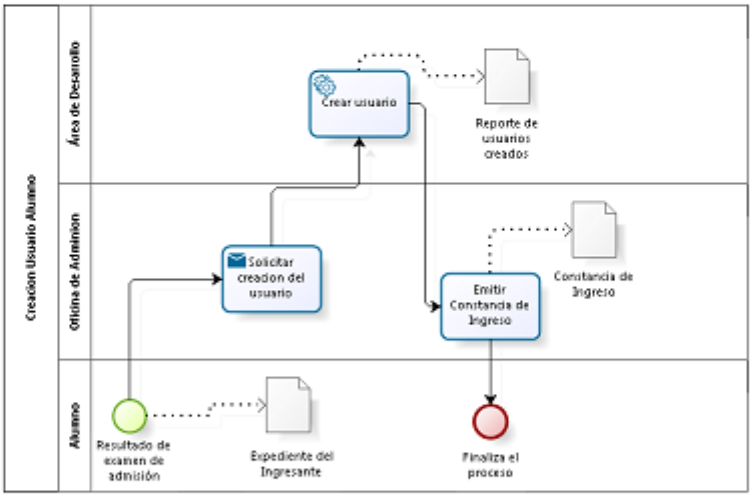


Fig.2 - Proceso de Creación de Usuario Alumno

Lista de Tareas		
Alumno	**Oficina de Admisión**	**Área de Desarrollo de Sistemas**
- Presenta el expediente donde indica sus datos personales.	**Solicitar Creación de usuario** - Enviar un correo solicitando la creación de usuario con los datos del nuevo docente.	**Crear el usuario:** - El área de desarrollo realiza la creación del usuario en base al

	Emitir constancia de Ingreso - Una vez obtenido el usuario y la contraseña del ingresante se imprime una constancia de ingreso con los datos respectivos.	reporte de alumnos ingresantes, por medio de un módulo del sistema académico.

Información General

Evento activador	El proceso se activa cuando un nuevo alumno ingresa a la Universidad por medio de alguna modalidad de ingreso
Objetivo	Establecer un procedimiento documentado, que informe y ayude en la gestión de las actividades de la creación de usuarios a alumnos ingresantes
Dueño	Área de Desarrollo Sistemas
Cliente	Oficina de Admisión

c) Tipo Usuario: Administrativo

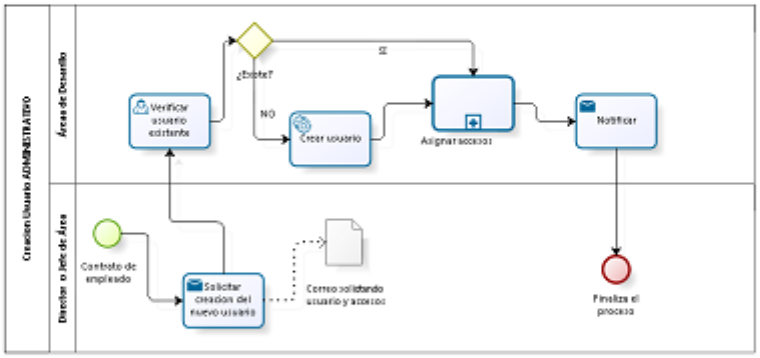


Fig.1 - Proceso de Creación de Usuario: Administrativo.

Lista de Tareas	
Director o Jefe de Área	**Área de Desarrollo de Sistemas**
Solicitar Creación de usuario ▪ Enviar un correo solicitando la creación de usuario con los datos del nuevo docente. ▪	**Verificar si existe:** ▪ Se realiza una consulta al sistema académico para revisar la existencia del usuario. .Si la condición es SI ▪ Se procede a signar accesos. Si la condición es NO: ▪ Se crea el usuario y luego se le asignan los accesos en un módulo propio del sistema Académico. Se notifica al director sobre la creación del usuario.

Evento activador	El proceso se activa cuando se contrata a un nuevo personal para laborar en un cargo administrativo.
Objetivo	Establecer un procedimiento documentado, que informe y ayude en la gestión de las actividades de la creación de usuarios administrativos y que usaran el Sistema Académico.
Dueño	Área de Desarrollo Sistemas
Cliente	Director de Área.

Roles participantes

- **Director o Jefe de área:** Realiza las solicitudes para la creación del usuario docente o administrativo cuando un nuevo personal es contratado; argumentando los accesos que debe tener de acuerdo a las responsabilidades propias del puesto de trabajo.
- **Área de Desarrollo de Sistemas:** Realiza el trabajo operativo de la creación de usuario mediante el Sistema Académico, así como la asignación de accesos.
- **Oficina de Admisión:** Presenta el reporte de ingresantes, y los emite junto a la constancia de ingreso.
- **Vicerrectorado:** Realiza las validaciones según el tipo de usuario a crear, en caso del docente que cumpla los requerimientos para ejercer la docencia.
-

Asignar accesos:
La asignación de accesos es un sub proceso que se activa cuando se solicita accesos o la creación de un usuario de tipo Administrativo, el cual puede ser catalogado de acuerdo al perfil o rol del puesto de trabajo:

Los perfiles se encuentran en la política de Gestión de Perfiles.

Glosario

- **Normativa**: Ley de Protección de datos personales (LPDP)
- **Usuario**: Persona que hace uso de un sistema informático, que encierra un conjunto de accesos y privilegios.
- **Acceso (Inf.):** Privilegios o permisos para ingresar a módulos restringidos del sistema Académico.
- **Administrativo:** Persona que laborará en la parte de la administración académica de la universidad, que requerirá información del sistema académico para el cumplimiento de sus funciones.

Tecnologías de apoyo

- Correo electrónico
- Teléfono celular
- Sistema Académico

Cumplimiento normativo

- Ley y Reglamento de Protección de Datos Personales.
- Estatuto UPeU
- Ley Universitaria-SUNEDU
- MOF

Indicadores principales

Número de usuarios creados sin autorización
Meta: 0
Periodo de evaluación: Fin de mes
Responsable: Área de Desarrollo

Historia de revisiones.

N° Versión	Fecha	Descripción de cambios
V1.0	07 de enero del 2018	Primera versión

Anexo 03

DIRECTRIZ DE CONTRASEÑAS SEGURAS

Directriz de contraseñas seguras		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: DSD009

Directriz de contraseñas seguras

Las sub áreas de Desarrollo de Sistemas y Mesa de Ayuda son los responsables de desarrollar y mantener el proceso de creación/modificación de un nuevo usuario respetando el Proceso de Gestión de Usuarios y Privilegios (**PRD-01**). Durante el desarrollo del proceso se mantendrá la confidencialidad de las contraseñas; se le comunicará al usuario evitar **guardar registros de papel**, se prohibirá que el sistema permita contraseñas vulnerables a ataques de diccionario y tengan caracteres consecutivos o repetitivos. Las contraseñas cumplirán con al menos:

-Ocho (8) digitos,

-Ser alfanuméricos y,

-En lo mínimo tendrá un carácter especial.

Al crear la cuenta de usuario a una persona, se le enviará un mensaje al correo electrónico previamente otorgado por la persona, donde se le facilitará la contraseña por defecto a cambiar con urgencia (cuando ingrese por primera vez le pedirá el cambio de contraseña).

Así mismo no se deberá mostrar la contraseña en la pantalla al introducirla. Las contraseñas se guardarán en forma cifrada.

DIGETI se reserva el derecho de modificar el presente documento para adaptarlo a cambios administrativos o legislativos.

Anexo 04

FORMATO DE DERECHOS DE ACCESO

Formato de derechos de acceso		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: DSD001

Yo..... en calidad de (alumno o colaborador) ....., con Nro. de DNI....., perteneciente a la facultad y/o área de estudio o trabajo ....., con cargo de (omitir si es estudiante) ....., **me comprometo a guardar y usar responsablemente los accesos que me son encomendados de acuerdo a la función y/o necesidad que implique mi persona en relación con la Universidad Peruana Unión.**

Fecha: ...../...../...../

_____

Firma

DIGETI se reserva el derecho de modificar el presente documento para adaptarlo a cambios administrativos o legislativos.

Anexo 05

FORMATO PARA EL PROGRAMA ANUAL DE AUDITORÍAS

	FORMATO	Código: DSD002
Una Institución Adventista	PROGRAMA ANUAL DE AUDITORÍAS	Versión: 1.0 Fecha: 01/02/2018 Empresa: Universidad Peruana Unión Área: DIGETI Aprobado: Director de DIGETI Elaborado: Equipo Investigador Página 1 de 1

Fecha de Actualización:	/ /
Año:	2018

No.	Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
1	Verificar el cumplimiento de la correcta asignación de accesos y privilegios												
2	Verificar el cumplimiento del acceso al centro de datos												
3	Verificar el cumplimiento de la autorización para la transferencia												
4	Verificar el cumplimiento del uso de la tecnología para la transferencia												
5	Comprobar la eficacia del procedimiento de recuperación												

Elaborado:	Aprobado:

Anexo 06

FORMATO PARA EL PLAN DE AUDITORÍAS INTERNAS

	FORMATO	Código: DSD003
Una Institución Adventista	PLAN DE AUDITORÍAS INTERNAS	Versión: 1.0 Fecha: 01/02/2018 Empresa: Universidad Peruana Unión Área: DIGETI Aprobado: Director de DIGETI Elaborado: Equipo Investigador
		Página 1 de 1

Auditor Líder: _____ FECHA: _____

Equipo Auditor: _____ _____

_____ _____

_____ _____

Alcance:

DÍA	HORARIO	Actividad	REQUISITOS ISO 27001 / LPDP	AUDITOR	AUDITADOS

_____ _____

ELABORADO POR: APROBADO POR:

Anexo 07

POLÍTICA ESPECÍFICA DE ALMACENAMIENTO Y RESPALDO

Política específica de Almacenamiento y Respaldo		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: PSD002

Política de Almacenamiento y Respaldo

1. Ante el almacenamiento de información de terceros alojado en el mismo espacio físico de DIGETI, se realizará un documento formal que especifique el trabajo que realizará el personal de DIGETI y el responsable ante cualquier incidente.
2. Realizar convenio con instituciones de la IASD para permitir realizar respaldos en sus sistemas de almacenamiento, cumpliendo así con la legislación y buenas prácticas.
3. Para toda realización de respaldos (Backup) se completará el Formato de Control de Backups (DSD005).
4. El formato DSD005 se revisará en las fechas acordadas según el Programa anual de auditoría (DSD002) y será ejecutado según el Plan de Auditorías Internas (DSD003).

DIGETI se reserva el derecho de modificar el presente documento para adaptarlo a cambios administrativos o legislativos.

Anexo 08

FORMATO DE CONTROL DE BACKUPS

FORMATO
CONTROL DE BACKUPS

DSD006
Versión: 1.0
Fecha: 01/02/2018
Aprob.: Director de DIGETI
Página 1 de 3

DESCRIPCIÓN	RUTA DE ACCESO	BASE DE DATO	FECHA Y HOR	RESPONSAB	FRECUENCIA	ESTADO	OBSERVACIONES

FORMATO
CONTROL DE BACKUPS

DSD006
Versión: 1.0
Fecha: 01/02/2018
Aprob.: Director de DIGETI
Página 2 de 3

AÑO:																																AÑO	
MES:	MES 1					MES 2					MES3					MES 4					MES 5						MES 6						
SEMANA:	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	6	1	2	3	4	5	1	2
TIEMPO DE CONSERVACIÓN																																	

FORMATO
CONTROL DE BACKUPS

DSD006
Versión: 1.0
Fecha: 01/02/2018
Aprob.: Director de DIGETI
Página 3 de 3

MES 7			MES 8					MES 9					MES 10						MES 11					MES 12				
3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	6	1	2	3	4	5	1	2	3	4	5

Anexo 09

FORMATO PARA EL RESUMEN DE VISITAS AL DATA CENTER

Resumen de visitas al Data Center								
Empresa: Universidad Peruana Unión				**Aprobado por:** Director de DIGETI		**Fecha:** 01/02/2018		
Área: DIGETI				**Elaborado por:** Equipo Investigador		**Versión:** 1.0	**Código:** DSD004	
Proveedor (Empresa)	**Nombre del Profesional**	**Persona de Contacto**	**Fecha y Hora de visita**	**Servicio o Equipo comprometido**	**Detalle**		**Objetivo de la visita**	**Observaciones**
					Acciones	**Compromiso (Fecha comprometida)**		
Optical Networks	Juan Perez	Anthony Calderon	18/05/2018 - 2:00 pm	Servicio internet	-Configuración de la red #### -Cambio de equipo	2:00 pm - 3:00 pm	Mejorar el servicio de internet	Demora en el servicio de configuración

Anexo 10

POLÍTICA ESPECÍFICA PARA LA TRANSFERENCIA DE DATOS

Política específica para la Transferencia de Datos		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: PSD003

Política para la Transferencia de Datos

1. Toda transferencia de datos fuera de la UPeU deberá ser autorizado por el Director de DIGETI (Responsable del Banco de Datos Lógico) respetando el formato para la autorización de traslado (DSD006) o con algún documento formal que especifique la empresa destinataria, finalidad, el soporte tecnológico de la transferencia u otros detalles según la confidencialidad de los datos.
2. Toda transferencia de datos donde se prestase servicios de alojamiento (nacional o extranjero) se deberá cumplir previamente con el Instructivo de gestión de acuerdos (DSD008), velando por un nivel alto de medidas de seguridad y cumplimiento de la Ley 29733.
3. Toda transferencia de datos será realizada con la tecnología API REST, sin embargo, se deberá seguir las recomendaciones de OWASP (Open Web Application Security Project) https://www.owasp.org/index.php/REST_Security_Cheat_Sheet.
4. Toda transferencia de datos (exitosa o no) deberá ser debidamente documentado en un formato simple para futuras auditorías.
5. La realización de auditorías se realizará según las fechas acordadas en el Programa anual de auditoría (DSD002) y será ejecutado según el Plan de Auditorías Internas (DSD003).

DIGETI se reserva el derecho de modificar el presente documento para adaptarlo a cambios administrativos o legislativos.

Anexo 11

FORMATO PARA LA AUTORIZACIÓN DE TRANSFERENCIA DE DATOS

Formato de mensaje vía e-mail para autorización de transferencia de datos		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: DSD006

El mensaje que enviara el Encargado del Banco de Datos deberá mantener la siguiente estructura para la autorización de la transferencia:

(Saludo)
Buenos días,

(Cuerpo)
Previa aprobación de Secretaría General, la presente es para autorizar el traslado del (o los) documento(s) con origen a la empresa (área institucional) xxxxx, la finalidad xxxxxxxxxx y con el soporte tecnológico xxxxxxxx de acuerdo a la política interna de transferencia de datos.

Muchas gracias.

(Texto adicional)
El presente mensaje sirve de evidencia para cualquier incidente que pueda ocurrir en el traslado.

Nota: En caso la transferencia implique el traslado externo a la organización se deberá enviar un mensaje con copia a rectorado.

Anexo 12

POLÍTICA ESPECÍFICA PARA EL ACCESO FÍSICO

Política específica para el Acceso Físico		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: PSD004

Política para el Acceso Físico

1. DIGETI supervisará y registrará las visitas al "Centro de Datos" por medio de un personal designado, el mismo que completará el documento de Resumen de visitas (DSD004).
2. La persona que solicite la visita tendrá acceso solo para propósitos específicos y autorizados. La visita se realizará por un periodo de tiempo definido de acuerdo al propósito.
3. Se prohibirá el uso de equipos de fotografía, video, audio u otra forma de registro al "Centro de Datos"; salvo lo requiera el personal (detallar en el formato DSD004) o por autorización del Responsable o Encargado del banco de datos lógico.
4. La puerta del "Centro de Datos" debe permanecer en todo momento cerrado. Así mismo el cuidado de las llaves y las tarjetas de acceso serán responsabilidad del Encargado del banco de datos lógico.
5. La realización de auditorías se realizará según las fechas acordadas en el Programa anual de auditoría (DSD002) y será ejecutado según el Plan de Auditorías Internas (DSD003).

Anexo 13

INSTRUCTIVO PARA LA GESTIÓN DE ACUERDOS

Instructivo para la gestión de acuerdo		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo Investigador	**Versión:** 1.0
		Código: DSD008

Anexo 14

COMPROMISO DE CONFIDENCIALIDAD

Compromiso de confidencialidad		
Empresa: Universidad Peruana Unión	**Aprobado por:** Director de DIGETI	**Fecha:** 01/02/2018
Área: DIGETI	**Elaborado por:** Equipo investigador	**Versión:** 1.0
		Código: OSD007

COMPROMISO DE CONFIDENCIALIDAD DE LOS EMPLEADOS EN CUANTO AL USO Y DIVULGACIÓN DE INFORMACIÓN

Fecha: _____

Nombres y Apellidos: _____

DNI: _____ Área de Trabajo: _____

Cargo del Empleado: _____

En mi capacidad de empleado (ya sea tiempo parcial o tiempo completo) y en consideración de la relación laboral que mantengo con la organización / empresa, así como del acceso que se me permite a sus bases de información (sistemas informáticos), constato que:

1. Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja mi empresa.

2. En concreto he leído, entiendo y me comprometo a cumplir los Procedimientos de Seguridad que corresponden a mi función en la empresa (descritos en la Política de Seguridad).

3. Me comprometo a cumplir, asimismo, todas las disposiciones relativas a la política de la empresa en materia de uso y divulgación de información, y a no divulgar la información que reciba a lo largo de mi relación con la empresa, subsistiendo este deber de secreto, aun después de que finalice dicha relación y tanto si esta información es de su propiedad, como si pertenece a un cliente de la misma, o a alguna otra organización que nos proporcione el acceso a dicha información, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.

4. Entiendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empresa y la posible reclamación por parte de la misma de los daños económicos causados.

_____

Firma Empleado/a

Anexo 15

DOCUMENTO DE RECOMENDACIONES

UNIVERSIDAD
PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

DOCUMENTO DE RECOMENDACIONES PARA LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN (DIGETI)

Equipo implementador	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Lima, Enero del 2018

El presente documento está elaborado en base a los Registros de Hallazgos (RD) de la evaluación realizada para identificar el nivel de cumplimiento de la Ley de Protección de Datos Personales en la UPeU-DIGETI, y para el mejoramiento de medidas de seguridad de la organización, las recomendaciones son las siguientes:

1. **Registro de Hallazgo-RD015**: Considerando que la UPeU actualmente está desarrollando un sistema ERP, es necesario que este software permita observar la **trazabilidad de los accesos** al sistema, tales como: horas de inicio, cierre de cesión, acciones relevantes y otros.
2. **Registro de Hallazgo-RD020**: Mejorar la **autenticación para el acceso al Data Center**, específicamente en el abastecimiento de las tarjetas para el personal y un mejor control de las mismas.
3. **Registro de Hallazgo-RD021**: Proteger los respaldos por **medios de encriptación** si el nivel de confidencialidad lo es requerido.
4. **Registro de Hallazgo-RD031, RD032**: Adquirir o desarrollar software o alguna tecnología que transporte información previa **encriptación** y posteriormente se verifique su integridad.

Anexo 10. Propuesta de controles para Secretaría General

UNIVERSIDAD
PERUANA UNIÓN
UNA INSTITUCIÓN ADVENTISTA

Propuesta de controles de seguridad para el cumplimiento de la Ley nro. 29733 en el área de Secretaría General

Equipo implementador	
Milton Tarrillo Villegas	miltontarrillo@upeu.edu.pe
Cristhian Calisaya Sana	cristhiancalisaya@upeu.edu.pe

Lima, Mayo del 2017

INDICE

I. GLOSARIO

Información: Es la interpretación que se le da a un conjunto de datos, puede estar de manera física como lógica.

Datos personales: Es aquella información que hace identificable a toda persona natural como: nombres, dirección, sexo, edad, etc.

Controles/Control: Es un mecanismo utilizado para asegurar un determinado servicio y/o activo. Los controles pueden ser procedimientos, formatos, tecnología, etc.

Incidente: Acceso o intento de acceso, uso, modificación o destrucción no autorizada de información que contenga datos personales o no.

Política: Es una guía orientada a la acción que debe ser divulgada, entendida y acatada por los miembros de una organización o área (siendo el caso de la investigación).

Política general: Es una guía a nivel de aplicación general, su impacto es alto y crítico.

Política específica: Es una guía con un nivel menor, determina ciertos procesos y es delimitado por su alcance.

Seguridad física: Es la aplicación de medidas para la protección de información ente amenazas de manera física o ambiental

Banco de datos físico: Es un conjunto de datos personales no automatizado

Tratamiento de datos personales: Es cualquier operación que permite la recolección, conservación, modificación o eliminación de datos personales.

Matriz RACI: Matriz de Asignación de Responsabilidades.

Trazabilidad: Es la capacidad de registro de las operaciones y/o actividades realizadas desde su origen hasta su destino.

Procedimiento: Es un modelo de conjunto de acciones que debe realizarse para lograr un objetivo.

Confidencialidad: Es el aseguramiento del acceso a documentos solo por personas autorizadas.

Integridad: Es el aseguramiento de información exacta, verídica y completa.

Disponibilidad: Es el aseguramiento de la información y/o servicio a las personas que lo requieran en todo momento.

II. INTRODUCCIÓN

La información se puede encontrar de forma digital o física, sin embargo, cual sea el caso es necesario adoptar medidas para asegurar su confidencialidad, integridad y disponibilidad.

Las actividades de almacenamiento, copia, acceso, traslado y prestación de servicios que refiera a datos personales, es una labor recurrente en el área de Secretaría General. Esta área realiza tratamiento de documentos administrativos, actas, resoluciones y entre otros archivos sensibles y relevantes que si sucede algún evento negativo pueda afectar considerablemente a la organización.

Por lo tanto, para mantener esta seguridad será necesario implantar controles que se adecuen al entorno organizacional, estas pueden ser: políticas, prácticas, procedimientos, estructuras organizativas, funciones de software y hardware, etc.

De igual forma para el cumplimiento de la Ley nro. 29733 (Ley de Protección de datos personales) en su apartado "Medidas de Seguridad" el presente documento propondrá controles de seguridad basados en la NTP-ISO/IEC 17799:2007, la cual ofrece recomendaciones para realizar una adecuada gestión de la seguridad de la información.

III. CUMPLIMIENTO DE LA METODOLOGÍA

Considerando el término de la primera y segunda etapa de la metodología que se muestra en la Figura 1;

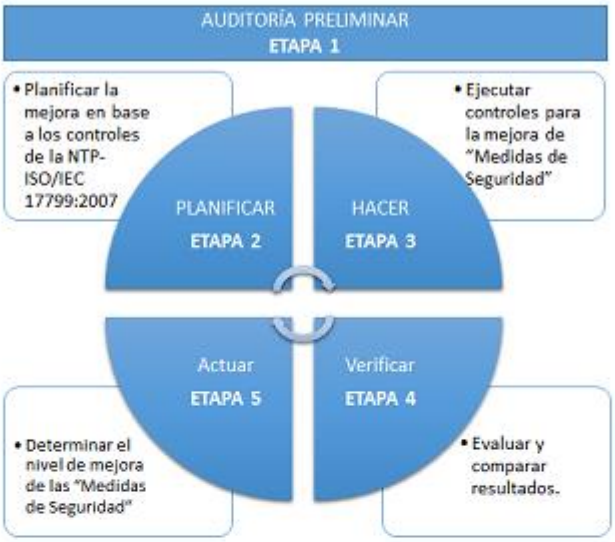


Figura1. Etapas de la metodología

Se procede a realizar las actividades pertenecientes a la tercera etapa *Ejecutar controles* que se contempla en la Figura 2.

Figura 2. Actividades para la ejecución de controles

IV. PROPUESTA DE CONTROLES DE SEGURIDAD

Basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007, la propuesta está estructurada en dos partes.

A. Control de seguridad general

La siguiente política general, refleja los controles específicos del presente documento. La política está desarrollada en base a la necesidad del área y la organización, por lo que se propone lo siguiente:

1. Política de seguridad física para la protección de datos

Código de propuesta: PS001	**Tipo**: Documento
Clausula: POLÍTICA DE SEGURIDAD	
Control: Documento de política de seguridad de la información.	
Alcance: La política general es aplicable a todo el personal de Secretaría General y trabajadores de la UPeU que realicen labores directamente con el área, también, a los usuarios externos que presten o prestare servicios al área. Implicará las actividades relacionados al (o la): 1. Almacenamiento, copia y acceso a la documentación no automatizada 2. Traslado de documentación no automatizada 3. Prestación de servicios sin acceso a datos personales	
Solución: Implementar una política general de seguridad física en Secretaría General, para dirigir y dar soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos del negocio, leyes y regulaciones. La política reflejará en absoluto los controles propuestos de la investigación.	
Documento adjunto: Ver el Anexo 01 para la política general.	

B. Control de seguridad específico

La propuesta de los siguientes controles se elaboró en base a los hallazgos encontrados en la evaluación previa y las cuales están reflejadas en la política general.

1. Almacenamiento, copia y acceso a la documentación no automatizada

1.1. Almacenamiento de documentación no automatizada

Esta actividad cumple con los predichos de la NTP-ISO/IEC 17799:2007, sin embargo, para fortalecer la seguridad proponemos seguir las recomendaciones del Anexo 02.

1.2. Copia o reproducción de la documentación no automatizada

1.2.1. Nombre de la propuesta: Matriz de asignación de responsabilidades (RACI)

Código de hallazgo: RS001	**Código de propuesta**: PS002
Descripción del hallazgo: Los trabajadores conocen sus responsabilidades por l experiencia en el puesto o alguna capacitación de su predecesor, mas no existe u documento que señale aquellas actividades encargadas y su negativa al incumplirlo.	
Clausula: ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Asignación de responsabilidades sobre seguridad de la información	**Tipo**: Documento
Alcance: El documento abarcará el personal en absoluto de Secretaria General. Señalará las funciones respecto a la seguridad física, el área se encargará de completar con las funciones propias al área.	
Solución: Implementar un documento que contenga el responsable, aprobador, consultado e informado de cada actividad perteneciente a Secretaría General, identificando claramente el activo o proceso que deberá velar y el efecto de incumplirla.	
Documento adjunto: Ver el Anexo 03 para la matriz de responsabilidades.	

1.2.2. Nombre de la propuesta: Destrucción planificada de documentos

Código de hallazgo: RS002	**Código de propuesta**: PS003
Descripción del hallazgo: Los documentos inválidos son almacenados en un lugar con fácil acceso. No se realiza una evaluación previa para ser reciclado.	
Clausula: GESTIÓN DE COMUNICACIÓN Y OPERACIONES	
Control: Eliminación de medios	**Tipo**: Tecnología y Procedimiento

Alcance: La máquina trituradora permanecerá en lugar determinado y su uso permitirá la eliminación de documentos de toda el área de Secretaria General. Existirá un responsable de dicha tarea.
Solución: Implementar un procedimiento que indique los responsables de la actividad, evitando destrucciones no planificadas y minimizando el riesgo de filtro de información sensible a personas externas con la eliminación segura. Adquirir una maquina destructora/trituradora de papel, para eliminar documentos de forma segura y sin peligro cuando no se necesiten más. Implementar un Registro de control de documentos a destruir para mantener la trazabilidad de los documentos que inicien con el procedimiento.
Documento adjunto: Ver el Anexo 04 para la destructora de papel, el Anexo 05 para el procedimiento y el Anexo 16 para el Registro de control.

1.3. Acceso a la documentación no automatizada

1.3.1. Para el hallazgo con código: **RS003**, que está relacionado con las responsabilidades que recae en el titular o responsable del banco de datos, se sugiere la propuesta de solución RACI (Matriz de asignación de responsabilidades) con código: **PR002.**

1.3.2. Nombre de la propuesta: Autorización y registro de accesos

Código de hallazgo: RS004, RS005, RS006 (Respectivamente).	**Código de propuesta**: PS004
Descripción del hallazgo: Los usuarios con acceso al área de datos no son autorizados por el encargado o titular del banco de datos mediante un documento de registro. Tampoco existe trazabilidad en los accesos al área de datos.	
Clausula: GESTIÓN DE COMUNICACIÓN Y OPERACIONES	
Control: Segregación de tareas	**Tipo**: Documento
Alcance: El documento se autorizará y registrará en el área de Secretaría General, sin embargo, los usuarios registrados y autorizados pueden implicar trabajadores externos al área y a la UPeU.	
Solución: Separar las tareas y áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional. El Secretario General como Encargado del Banco de Datos autorizará tales segregaciones. Los documentos a implementar serán los siguientes: • Formato para la autorizar o retirar el acceso de usuarios al área de datos. • Formato para registrar la lista de usuarios autorizados a los datos personales. • Formato para mantener la trazabilidad del acceso al área de datos (persona, fecha, motivo, etc.)	
Documento adjunto: Ver el Anexo 06 para el formato de autorización, Ver el Anexo 07 para el formato de registro y Ver el Anexo 08 para el formato de trazabilidad del	

acceso.

2. Traslado de documentación no automatizada

2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado

2.1.1. Nombre de la propuesta: Aseguramiento en el traslado de documentos

Código de hallazgo: RS007, RS008, RS009, RS010 Y RS011 (Respectivamente).	**Código de propuesta**: PS005
Descripción del hallazgo: No existe un registro de las autorizaciones de traslado de documentos encargado por un responsable (Secretario General). Así mismo, no hay un registro para los usuarios y mensajeros autorizados a trasladar y su trazabilidad para el envió. Sabiendo que en su mayoría la información que trata Secretaría General es sensible, no se cuenta con mecanismo adicional de seguridad para su traslado.	
Clausula: GESTIÓN DE COMUNICACIÓN Y OPERACIONES	
Control: Medios físicos en tránsito	**Tipo**: Documento
Alcance: Los controles propuestos solo se usarán en el área de Secretaría General. El sobre para la transferencia de documentos sensibles no podrá ser usado para otras finalidades.	
Solución: Implementar documentos y procedimientos para proteger los medios contra personal no autorizado, mal uso o corrupción durante el transporte de los documentos de Secretaría General. Los documentos serán los siguientes: • Formato de una solicitud para la autorización del traslado de documentos que contengan datos personales, aprobado por el encargado o titular del banco de datos. • Formato para el registro de usuarios y/o mensajeros autorizados o no para trasladar datos personales. • Formato para mantener la trazabilidad ante usuarios y/o mensajeros autorizados para trasladar. • Implementar una política específica para el traslado de documentos.	
Documento adjunto: Ver el Anexo 07 para el registro, Ver el Anexo 08 para la trazabilidad, Ver el Anexo 09 para la solicitud de autorización, Ver el Anexo 10 para la política específica.	

2.2. Eventos o incidentes en el traslado de datos personales

2.2.1. Nombre de la propuesta: Notificación y respuesta ante incidentes

Código de hallazgo: RS012, RS013, RS014 (Respectivamente).	**Código de propuesta**: PS006
Descripción del hallazgo: Durante las tareas comunes en el área, suceden incidentes de seguridad (Área de datos). Al ocurrir estos eventos, no existe un documento formal que facilite la respuesta a los incidentes. De la misma forma, estos eventos no suelen ser registrados ni notificados a la administración o al titular de los datos personales.	
Clausula: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
Control: Reportando los eventos en la seguridad de información	**Tipo**: Procedimiento y Documento
Alcance: La extensión del reporte de eventos y su respuesta abarcará el área de Secretaría General, la administración y la persona afectada directamente.	
Solución: Implementar un procedimiento de reporte de eventos junto con una respuesta a incidentes, estableciendo las acciones y los responsables que Secretaría General deberá tomar en cuenta al recibir dicho reporte. Los procedimientos y documento son los siguientes: • Formato para el registro y respuesta de los incidentes de seguridad relacionada al acceso o manipulación en el traslado. • Procedimiento para la notificación (en caso lo requiera) a la gerencia. • Procedimiento para la notificación al titular o titulares de los datos personales.	
Documento adjunto: Ver el Anexo 11 para el formato del registro, Ver el Anexo 12 para el procedimiento de notificación sea el caso de dirigirse a la gerencia o al titular de los datos personales.	

3. Prestación de servicios sin acceso a datos personales

3.1. Servicios internos de la organización o área sin acceso a datos personales

3.1.1. Nombre de la propuesta: Política específica de control físico

Código de hallazgo: RS015, RS016, RS017 (Respectivamente).	**Código de propuesta**: PS007

Descripción del hallazgo: Actualmente en Secretaría General no existe un documento que límite la utilización de equipos de registro, realización de trabajos y acceso de personal interno (UPeU) al área, en especial al "Área de datos".	
Clausula: SEGURIDAD FÍSICA Y DEL ENTORNO	
Control: Controles físicos de entradas	**Tipo**: Documento
Alcance: La política será al nivel de área (política específica). El personal de Secretaría General y demás áreas de la UPeU que deseen acceder al área de datos deberán cumplir la política.	
Solución: Implementar una política específica donde señale detalladamente quienes son las personas autorizadas al área de datos. Se supervisará y monitoreará las visitas al Área de Datos. El documento cumplirá con lo siguiente: • Limitar el acceso del personal ajeno al área a documentos que contengan datos personales. • Limitar la realización de trabajos que no impliquen el tratamiento de datos personales. • Restringir el uso de equipos de fotografía, video, audio u otra forma de registro en el área de datos, salvo autorización del titular del banco de datos personales o encargado.	
Documento adjunto: Ver el Anexo 13 para la política de control físico.	

3.2. Servicios externos a la organización sin acceso a datos personales

3.2.1. Nombre de la propuesta: Seguridad en la gestión de acuerdos

Código de hallazgo: RS018, RS019, RS021	**Código de propuesta**: PS008
Descripción del hallazgo: Existe una deficiencia al gestionar la seguridad en la contratación de servicios externos. Teniendo en cuenta la labor que realizaran por medio de cláusulas contractuales o documentos que respalden su seguridad.	
Clausula: ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Identificación de riesgos por el acceso de terceros	**Tipo**: Administrativo
Alcance: Se brindará las actividades a realizar ante la prestación de servicios de terceros. El impacto será solo en el área de Secretaría General.	
Solución: Gestionar acuerdos (contractuales y/o legales) donde los terceros que presten servicios a Secretaría General estén enterados de sus obligaciones y responsabilidades que implique acceder, procesar, comunicar o manejar la información de la organización (área de datos).	

Documento adjunto: Ver el Anexo 14 para observar las directrices a cumplir para gestionar acuerdos con terceros.

3.2.2. Nombre de la propuesta: Acuerdo de confidencialidad

Código de hallazgo: RS020	**Código de propuesta**: PS009
Descripción de hallazgo: El personal interno de Secretaría General no cuenta con un documento donde describa la confidencialidad que deberá guardar durante la prestación de sus servicios. El personal realiza sus labores sin declarar el compromiso que tendrá al tratar con documentos que contengan datos personales.	
Clausula: ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	
Control: Acuerdos de confidencialidad	**Tipo**: Documento
Alcance: El documento de acuerdo de confidencialidad será validado por el área de Recursos Humanos para ser aplicado en el área de Secretaría General.	
Solución: Implementar un documento contractual para los empleados de Secretaría General donde acepten y firmen los términos y condiciones del contrato del empleo. El documento también considerará las responsabilidades, derechos y las acciones que se ha de tomar en caso incumpla el acuerdo durante el periodo de tiempo definido.	
Documento adjunto: Ver el Anexo 15 para el acuerdo de confidencialidad.	

V. ANEXOS

ANEXO 01

POLÍTICA DE SEGURIDAD FÍSICA PARA LA PROTECCIÓN DE DATOS PERSONALES

POLITICA DE SEGURIDAD PARA LA PROTECCION DEL BANCO DE DATOS NO AUTOMATIZADO

UNIVERSIDAD PERUANA UNIÓN

SECRETARÍA GENERAL

Importante: Secretaria General se reserva el derecho de modificar la presente política para adaptarla a cambios administrativos o legislativos.

INFORMACIÓN DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
_____	_____	_____
Equipo Investigador	Asesor Legal de Secretaría General/I Secretario General	Secretario General

CONTROL DE VERSIONES				
Nº Revisión	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
0(Cero)	24/04/2017	Elaboración inicial	Todas	Equipo Inv.
1				
2				
3				

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El área de Secretaría General es un órgano[1] encargado de dar apoyo académico y administrativo a toda la estructura orgánica de la Universidad Peruana Unión (UPeU).

Dentro de sus unidades administrativas (o sub áreas), la Secretaría General está constituida por: Trámite documentario, Grados y títulos, Archivo académico general, Carnés universitarios, Estadística e información, Registros y actas académicos y administrativos.

La Secretaría General entiende la importancia de proteger la información, reconociendo a este como un activo para la organización y también la obligación de cumplir con la Ley de Protección de Datos Personales (LPDP) a nivel organizacional. Que en efecto disminuirá los incidentes relacionados a la seguridad de la información, ofreciendo un mejor servicio en función de nuestras facultades como Secretaría General de acuerdo al estatuto de la UPeU.

Por ello, se establece la presente política para regular y asegurar el manejo de la información durante el proceso de su tratamiento en el área (almacenamiento, copia, acceso, traslado y prestación de servicios y otros) de los datos personales.

Esta política general está constituida en base a los lineamientos de seguridad descritos por la NTP-ISO/IEC 17799:2007, de acuerdo a la necesidad del negocio de la organización y los requerimientos de la LPDP.

1. Estatuto, Resolución Nº052-2014/UPeU-AU

2. BJETIVOS

La presente política para la protección de datos personales físicos tiene los siguientes objetivos:

- Proteger la información de la organización encontrada en el área conservando los atributos de confidencialidad, integridad y disponibilidad.
- Controlar las actividades que refiere a la seguridad de la información y sus responsables.
- Mejorar la calidad de servicio en la gestión documentaria (diligencias y transferencias).
- Gestionar las actividades de proveedores de servicios para mantener un nivel de seguridad óptimo.
- Promover una cultura de seguridad de la información.
- Cumplir con la Ley de Protección de Datos Personales en la UPeU.

3. ALCANCE

Esta política se aplica a todo el personal de Secretaría General y el personal de la UPeU que realice labores directamente con el área, y también a usuarios externos que presten o prestaren servicios al área. Así mismo, implica las actividades relacionadas al (o la):

- Almacenamiento, copia y acceso a la documentación no automatizada
- Traslado de documentación no automatizada
- Prestación de servicios sin acceso a datos personales.

Enfatizando el acceso al Área de Datos (Archivo Académico), la cual contiene información fidedigna y critica para la UPeU.
La política abarca el cumplimiento de la Ley de Protección de Datos Personales para el capítulo IV "Medidas de Seguridad", en específico lo relacionado a la seguridad física, considerando los controles de seguridad de acuerdo a la necesidad del área y la organización, recomendados por la NTP-ISO/IEC 17799:2007, un documento que ofrece una adecuada gestión de la seguridad de la información. Las clausulas son las siguientes:

- Aspectos organizativos para la seguridad
- Gestión de comunicación y operaciones
- Gestión de incidentes en la seguridad de la información
- Seguridad física y del entorno
- Política de seguridad

4. DEFICINICIONES Y TÉRMINOS

Información: Es la interpretación que se le da a un conjunto de datos, puede estar de manera física como lógica.

Datos personales: Es aquella información que hace identificable a toda persona natural como: nombres, dirección, sexo, edad, etc.

Incidente: Acceso o intento de acceso, uso, modificación o destrucción no autorizada de información que contenga datos personales o no.

Política: Es una guía orientada a la acción que debe ser divulgada, entendida y acatada por los miembros de una organización o área (siendo el caso de la investigación).

Política general: Es una guía a nivel de aplicación general, su impacto es alto y crítico.

Política específica: Es una guía con un nivel menor, determina ciertos procesos y es delimitado por su alcance.

Banco de datos físico: Es un conjunto de datos personales no automatizado

Tratamiento de datos personales: Es cualquier operación que permite la recolección, conservación, modificación o eliminación de datos personales.

Matriz RACI: Matriz de Asignación de Responsabilidades.

Documento inválido: Es un documento obsoleto, no utilizable o innecesario, potencialmente a ser eliminado.

Trazabilidad: Es la capacidad de registro de las operaciones y/o actividades realizadas desde su origen hasta su destino.

Procedimiento: Es un modelo de conjunto de acciones que debe realizarse para lograr un objetivo.

5. RESPONSABILIDADES Y CUMPLIMIENTO

5.1. RESPONSABILIDADES

Responsable del Banco de Datos Físico: Secretario General.

Encargado del Banco de Datos Físico: Secretaria de archivo académico general

Responsable del proceso de notificación de incidentes: Jefe de estadística e informática

Responsable del proceso de destrucción de documentos: Secretaria de registros y actas administrativas y académicos

Encargado de la transferencia de datos personales: Secretaria de trámite documentario

Consultor y Asesor: Asesor legal de Secretaria General

5.2. CUMPLIMIENTO

La presente política, entra en vigencia una vez aprobado por el Secretario General y dado el visto bueno por el asesor legal del área.

El trabajador que ingrese al área con posterioridad a la fecha de aprobación, se le entregará una copia del presente documento y así mismo deberá declarar su conocimiento y aceptación con una firma.

La política está alineada a las necesidades propias del área y la organización, como también a la legislación existente (LPDP), cualquier cambio administrativo, organizacional o respecto a la normatividad se deberá informar inmediatamente al responsable del documento.

6. POLÍTICA

6.1. ALMACENAMIENTO, COPIA Y ACCESO A LA DOCUMENTACIÓN NO AUTOMATIZADA

- Las tareas de almacenamiento, copia y acceso de documentos que contengan datos personales será realizado por un responsable, según lo expresado en el presente documento (En el apartado 5.1) y la matriz RACI (DSF003).
- Los documentos inválidos serán debidamente eliminados, respetando el Procedimiento de destrucción de documentos (PRS-02), el formato (DSF004) y utilizando la máquina trituradora.
- Se autorizará y registrará los accesos de los usuarios al Área de Datos manteniendo el formato (DSF007), así mismo, se completará un formato para mantener la trazabilidad de cada visita al área mencionada (DSF002).
- Para toda visita al Área de Datos se cumplirá la Política específica física de entrada (PSF003).

6.2. TRASLADO DE DOCUMENTACIÓN NO AUTOMATIZADA

- Toda transferencia o traslado de documentos fuera de las oficinas de Secretaría General o de la organización se realizará de acuerdo a la Política específica de traslado (PSF002)
- La transferencia o traslado de documentos será registrado (DSF001), autorizado (DSF006) y dado seguimiento (DSF002) de acuerdos a los formatos, y realizado por un responsable según lo expresado en el presente documento y la matriz RACI (DSF003).
- Los incidentes o eventos relacionados con la seguridad o vulneración de documentos serán notificados respetando el Procedimiento de Notificación (PRS-01).
- Los incidentes relacionados a la documentación física se deberán completar con el formato de Reporte de Incidentes (DSF005) con antelación y objetividad.

6.3. PRESTACIÓN DE SERVICIOS SIN ACCESO A DATOS PERSONALES

- El responsable de limitar el acceso deberá estar registrado en la matriz RACI (DSF003).
- Todo trabajo que implique el acceso de terceros al Área de Datos deberá cumplir con la Política de física de entrada (PSF003)
- Toda contratación de servicios que implique tratamiento de documentos se deberá realizar según las especificaciones del documento gestión de acuerdos (DSF009).
- Todo el personal de Secretaría General deberá declarar su entendimiento y aceptación mediante una firma sobre el acuerdo de confidencialidad (DSF008).

ANEXO 02

RECOMENDACIONES PARA EL ALMACENAMIENTO FÍSICO

Recomendaciones para el almacenamiento de la documentación física según la NTP-ISO/IEC 17799:2007:

Cláusula: SEGURIDAD FÍSICA Y DEL ENTORNO

Control: Perímetro de seguridad física

1. Las puertas del Área de datos deberán estar cerradas con llave cuando estén desatendidas.
2. Implementar un protocolo para la operación contra incendios, contemplando los reglamentos otorgados por DEFENSA CIVIL.
3. Adquirir un extintor o extintores (según sea la necesidad) para dar respuesta a los incendios.
4. El responsable del área de Grados y Títulos deberá ser un medio de control de acceso físico al Área de datos, evitando accesos no autorizados.
5. Instalar un sistema de alarma para la detección de intrusos, y probar su funcionamiento mensualmente.

ANEXO 03

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

1. Instrucciones

Matriz de Asignación de Responsabilidades (RACI)

Instrucciones

Elaborado por: Equipo Investigador

Actividades y colaboradores

Columna	Instrucciones
Activo/Proceso	Se ingresa aqui el identificador (ID) de la actividad de proyecto, con el mismo número utilizado para identificar la actividad o paquete de trabajo en los documentos de proyecto.
Actividad	Se coloca el nombre completo de la actividad (Por ej. "Realizar levantamiento de información", "Almancenar Grados y Titulos", "Elaborar actas").
Persona	Completar con el nombre y apellido de la persona responsable de la acticidad, adicionando entre parentesis el área que representa(Ejem. José Tipa (Auditor interno))
Roles / Responsabilidades por Actividad	En cada renglón (fila) especificar el tipo de responsabilidad asociado al colaborador de la columna, con los siguientes valores posibles: **R:** Responsable, **A:** Aprobador, **C:** Consultado, **I:**

Roles y Responsabilidades

Rol / Responsabilidad	Descripción
R	**Responsable:** Este rol es el que realiza (ejecuta) el trabajo asociado con la actividad, lo habitual es que cada actividad tenga un solo "R", si existe más de uno es recomendable subdividir la actividad.
A	**Aprobador:** Es el encargado de aprobar (firmar), el trabajo realizado, a partir de esa aprobación, este se vuelve responsable por la actividad. Como regla general debe existir un solo "A" por actividad. Este rol es quien asegura que se ejecutan las tareas, por ejemplo Lideres de área técnica, área de gestión de proyecto, entre otros.
C	**Consultado:** Posee alguna información o capacidad que se necesita para mantener el trabajo. Se le informa y consulta información, de manera bidireccional con el responsable y/o aprobador.
I	**Informado:** Rol que debe ser informado sobre el progreso y los resultados del trabajo. En este caso la comunicación es unidireccional (se le da información pero no se recibe información).

2. Matriz

Matriz de Asignación de Responsabilidades (RACI)

Elaborado por: Equipo Investigador

Roles / Responsabilidades: **R:** Responsable, **A:** Aprobador, **C:** Consultado, **I:** Informado.

Responsabilidad		Roles / Responsabilidades							
Activo/Proceso	Actividad	Secretario General (Edgar Horna)	Estadístico 1(Pxd)	Asistente Legal (Wilberth Gonzales)	Persona 1 (Archivo Institucional)	Persona 2 (Registro Administrativo)	Persona 3 (Registro Académico)	Persona 4 (Grados y Títulos)	Persona 5 (Trámite Documentario)
Proceso: Autorización a personal interno y externo	Designar y revocar autorizaciones a personal interno y externo al área de datos Designar y revocar accesos a personal interno y externo al área de	A	R	C					
Proceso: Registro de usuarios autorizados	Registrar los usuarios autorizados o no al área de datos Mantener en funcionamiento del documento de registro	I			R				
Proceso: Registro de accesos	Registrar los accesos (visitas) al área de datos, siguiendo el detalle Mantener en funcionamiento del documento de registro	I			R				
Activo: Fotocopiadora	Velar por el cuidado y el buen uso de la fotocopiadora perteneciente al subárea	A			R	R	R	R	R
Activo: Maquina destructora de papel	Velar por el cuidado y el buen uso de la maquina perteneciente al área	A	R	C	I				
Proceso: Destrucción de copias desechas	Mantener el cumplimiento del proceso de "Destruoción de copias"	A	R	C		I	I	I	
Proceso: Supervisar copias	Supervisar en todo momento el proceso de reproducción de documentos Retirar documentos originales y copias inmediatamente del equipo	I	R		R	R	R	R	R
Proceso: Traslado de documentos	Autorizar el traslado de documentos de forma física y lógica	A							R
	Autorizar y retirar accesos a usuarios/mensajeros para trasladar	A							R
Proceso: Registro para y durante el traslado	Registrar los usuarios/mensajeros autorizados o no para trasladar documentos Registrar la trazabilidad de usuarios/mensajeros cuando se trasladen documentos Mantener el funcionamiento del documento de registro	A		o		R		R	R
Proceso: Respuesta a incidentes	Mantener el cumplimiento del proceso de "Respuesta a incidentes"	A	R	C	R	R	R	R	R
Proceso: Respuesta a incidentes	Registrar incidentes en el traslado de documentos		R						
Proceso: Notificación de incidentes	Notificar incidentes al titular de los datos personales cuando sea necesario	A		C			R		
	Notificar incidentes a Rectorado cuando sea necesario	A		C			R		
Proceso: Limitar el acceso personal y de equipos	Limitar el acceso al personal de la UPoU al área de datos		C		R				
	Limitar la realización de trabajos que no impliquen datos personales		C		R				
	Restringir el uso de equipos de registro al área de datos (Cámara fotográfica, video, audio u otros)		C		R				
Proceso: Gestionar clausulas y/o contratos	Gestionar clausulas o documentos contractuales que regulen la prestación de servicios externos	A		C					

Nota: Los nombres inscritos en la matriz pertenecen a la fecha que se realizo la investigación.

3. Acciones por Incumplimiento

Acciones por incumplimiento de responsabilidades

Elaborado por: Equipo Investigador

Actividades y colaboradores

Gravedad	Características de la infracción	Acciones administrativas
Leve	- De 3 (tres) a 5 (cinco) tareas o actividades realizada parcialmente o deficiente	Llamada de atención
(*)Moderado	-Transferir documentos sin autorización del encargado del banco de datos. -Permitir acceder a personas no autorizadas al área de datos	Memorandum
(*)Grave	-Lucrar o beneficiarce con los accesos otorgados.	Comunicación a la administración. Cambio de puesto.

Se considerará la gravedad a partir de la primera falta o infracción

ANEXO 04

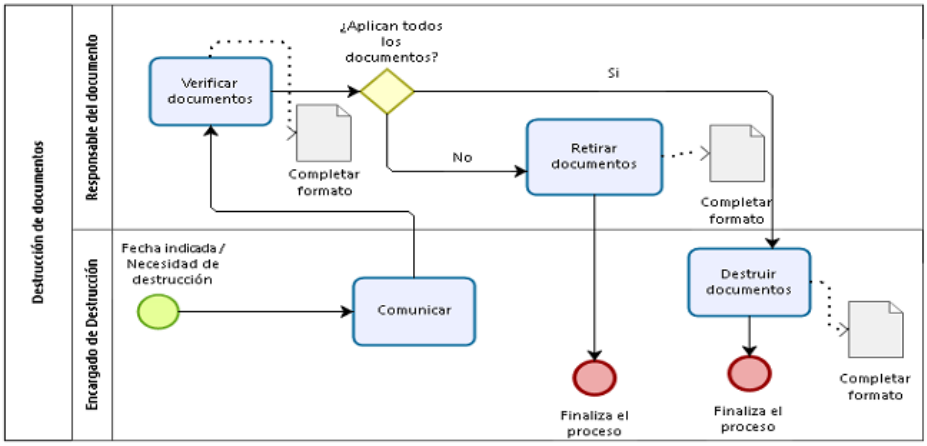
PRESUPUESTO PARA ADQUIRIR UNA TRITURADORA DE PAPEL

Modelo	JP-812S
Uso	Personal
Tamaño de corte	Tiras 4 mm
Destrucción por día	100 hojas
Hojas por vez	8
También destruye	T/C – Grapas
Depósito	21 litros
Ranuras ingreso	1
Tamaño ingreso	230 mm
Nivel de ruido	68 db bajo
Peso	7.5 kg.
Dimensiones	38.x.27.5.x 43.5 Cm

Costo Aproximado: S/. 370

ANEXO 05

PROCEDIMIENTO PARA LA DESTRUCCIÓN DE DOCUMENTOS



ANEXO 06

FORMATO PARA OTORGAR Y RETIRAR ACCESOS AL ÁREA DE DATOS

Formato para otorgar y retirar accesos al Área de Datos		
Empresa: Universidad Peruana Unión	Aprobado por: Secretario General	Fecha: 01/04/2017
Área: Secretaría General	Elaborado por: Equipo Investigador	Versión: 1.0

Yo..... como Secretario General y Encargado del Banco de datos con las facultades que me corresponden de acuerdo al Estatuto y la normatividad peruana, doy por *(otorgado o retirado)* ..... a la persona con Nombres y Apellidos ....., con DNI....., perteneciente al Área de ....., teniendo el cargo de ....., tales accesos:

1. Accesos para la documentación física:

Acceso 1	( )		*Acceso 6*	( )	
Acceso 2	( )		*Acceso 7*	( )	
Acceso 3	( )		*Acceso 8*	( )	
Acceso 4	( )		*Acceso 9*	( )	
Acceso 5	( )		*Acceso 10*	( )	

2. [*]Justificación:

Teniendo como argumento por lo siguiente:

_____

_____

_____

_____

Fecha: ..../.../.../

_____

Firma y Sello del
Secretario General

***Adjuntar documento en caso exista alguno que lo justifique**

ANEXO 07

FORMATO PARA REGISTRAR USUARIOS/PERSONAS O EMPRESAS AUTORIZADOS O NO AL ACCESO Y/O TRASLADO

Formato para el Registro de usuarios autorizados		
Empresa: Universidad Peruana Unión	**Aprobado por:** Secretario General	**Fecha:** 01/04/2017
Área: Secretaría General	**Elaborado por:** Equipo Investigador	**Versión:** 1.0

Nº	Nombres y Apellidos (o Nombre Empresa)	Documento de Identidad (o RUC)	Área (o Dirección)	Cargo (o Telefono)	Motivo	Estado	Tipo (Acceder o Trasladar)
1	Juan Perez	87876765	Acreditación	Director	Cumplir con la acreditación	Autorizado	Trasladar
2	Carlos Vergara	89012456	DIGETI	Asistente	Uitilizar camara fotografica	No Autorizado	Acceder
3	Transporte Gacela	98761200981	Av. Elmer Faucett 3481	575-3728	Envio a Provincia	Autorizado	Trasladar

ANEXO 08

FORMATO PARA MANTENER LA TRAZABILIDAD DEL ACCESO Y TRASLADO DE DOCUMENTOS

Formato para la trazabilidad del acceso y el traslado de documentos		
Empresa: Universidad Peruana Unión	**Aprobado por:** Secretario General	**Fecha:** 01/04/2017
Área: Secretaría General	**Elaborado por:** Equipo Investigador	**Versión:** 1.0

Nº	Nombres y Apellidos (o Nombre Empresa)	Nº de Oficio o TUPA	Motivo	Área/Cargo (o Dirección)	Hora Entrada (o Envio)	Hora Salida (o Llegada)	Fecha	Nombre del Encargado	Observaciones	Tipo (Acceder o Trasladar)
1	Juan Perez	TUPA001-452241	Cumplir con la acreditación	Acreditación	3:00 PM	3:30 PM	10/01/2017	Paul	Ninguna	Trasladar
2	Carlos Vergara	TUPA002-334241	Uitilizar camara fotografica	DIGETI	2:30 PM	3:00 PM	15/01/2017	Jack	Tiempo excedido	Acceder

Importante: Para el envio de información sensible se debera usar: Contenedores cerrados y/o Entrega en mano y/oEnvase con detección de apertura (Señalar el mecanismo en observaciones)

ANEXO 09

FORMATO PARA LA AUTORIZACIÓN DEL TRASLADO FÍSICO POR EL ENCARGADO

Formato de mensaje vía e-mail para autorización de traslado		
Empresa: Universidad Peruana Unión	**Aprobado por:** Secretario General	**Fecha:** 01/04/2017
Área: Secretaría General	**Elaborado por:** Equipo Investigador	**Versión:** 1.0

El mensaje que enviara el Encargado del Banco de Datos deberá mantener la siguiente estructura para la autorización de la transferencia:

(Saludo)
Buenos días estimado,

(Cuerpo)
Mediante la presente autorizo el traslado del (o los) documento(s) para ser trasladados con origen xxxxx, la finalidad xxxxxxxxxxxxxxxxxxxxxx. El responsable del traslado es la persona xxxxxxxxxxxxxxxxxx con cargo xxxxxxxxxxxxxxxxx perteneciente al área xxxxxxxxxxxxxxxx.

Gracias.

(Texto adicional)
El presente mensaje sirve de evidencia para cualquier incidente que pueda ocurrir en el traslado.

Nota: En caso la transferencia implique el traslado externo a la organización se deberá enviar un mensaje con copia a rectorado.

ANEXO 10

POLÍTICA ESPECÍFICA PARA EL TRASLADO DE DOCUMENTOS

Política específica de traslado de documentos		
Empresa: Universidad Peruana Unión	**Aprobado por:** Secretario General	**Fecha:** 01/05/2017
Área: Secretaria General	**Elaborado por:** Equipo Investigador	**Versión:** 1.0

Política de traslado de documentos

Ante todo traslado de documentos (externos e internos) que contengan datos personales, se autorizará, controlará y ejecutará el traslado en base a la matriz RACI. Se deberá seguir el formato de solicitud para la autorización del traslado de documentos por el encargado o titular del banco de datos (Correo o algún otro documento registrado).

Ante el traslado de documentos a las afueras de las instalaciones de la organización se deberá usar realizar solo los usuarios y/o mensajeros autorizados para el traslado, de igual manera, se deberá registrar y supervisar la trazabilidad del traslado según la matriz RACI.

ANEXO 11

FORMATO PARA EL REGISTRO Y RESPUESTA A INCIDENTES DE SEGURIDAD

Formato para el registro de incidentes		
Empresa: Universidad Peruana Unión	Aprobado por: Secretario General	Fecha: 01/09/2017
Área: Secretaría General	Elaborado por: Equipo investigador	Versión: 1.0

Fecha y Hora del llenado del reporte:

1. DATOS GENERALES

Llene esta parte con los datos personales de la persona que está llenando el reporte.

Nombre del trabajador: _____

DNI: _____ Sub área: _____ Celular: _____

Cargo: _____ Correo electrónico: _____

2. DESCRIPCIÓN DEL INCIDENTE

Fecha: _____ Hora:_____Lugar: _____

Qué actividad se encontraba realizando:

_____
_____
_____
_____

3. DESCRIPCIÓN DE LOS HECHOS (¿Donde sucedió? ¿Cómo sucedió?)

_____
_____
_____

4. POSIBLES CAUSAS

_____
_____
_____
_____
_____
_____
_____
_____
_____

5. ACCIONES CORRECTIVAS

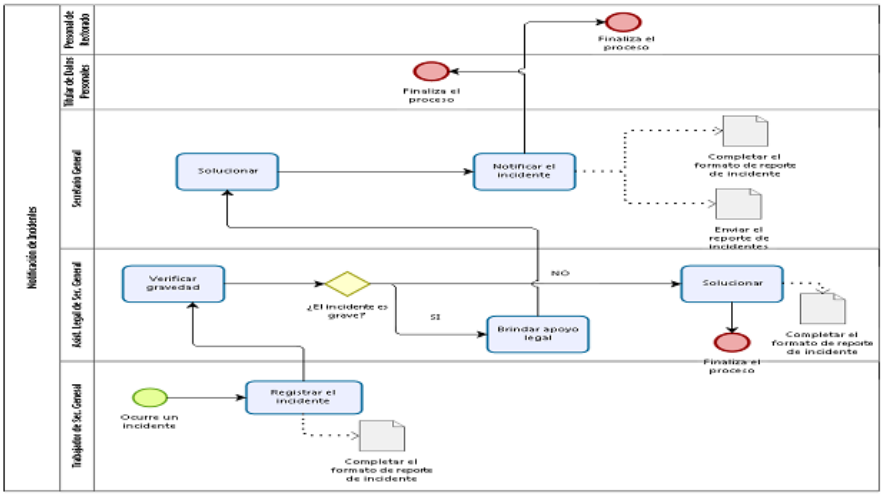
_____
_____
_____
_____
_____
_____
_____
_____
_____

6. OTROS CONTACTOS

Nombres/Información de contactos que apoyen a la investigación del incidente
Nombres y Apellidos: Datos de contacto:
Nombres y Apellidos: Datos de contacto:

ANEXO 12

PROCEDIMIENTO DE NOTIFICACIÓN DE INCIDENTES



ANEXO 13

POLÍTICA ESPECÍFICA DE CONTROL FÍSICO DE ENTRADA

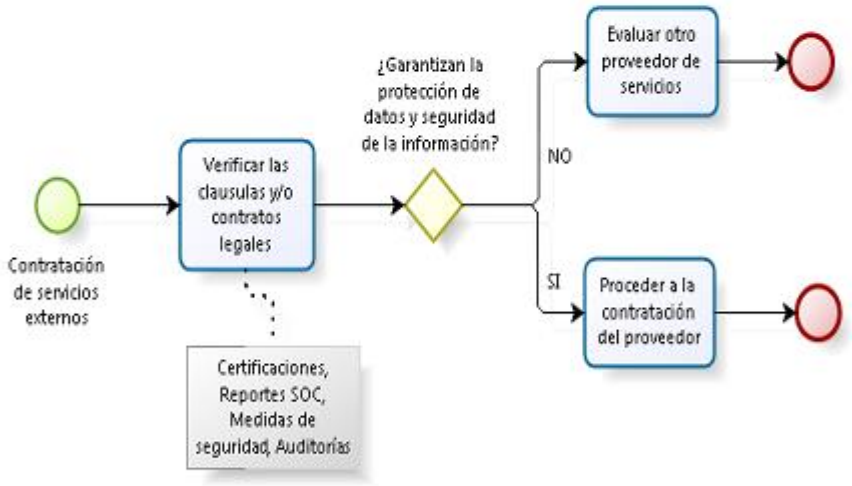
Política específica de control físico de entrada		
Empresa: Universidad Peruana Unión	Aprobado por: Secretario General	Fecha: 01/02/2017
Área: Secretaría General	Elaborado por: Equipo Investigador	Versión: 1.0

Política de control físico de entrada

Secretaría General supervisará y registrará las visitas al "Área de datos" por medio de un personal designado apoyándose en el registro de personas autorizadas y no autorizadas. La persona que solicite la visita tendrá acceso solo para propósitos específicos y autorizados. Se prohibirá el uso de equipos de fotografía, video, audio u otra forma de registro al "Área de datos"; salvo autorización del encargado del banco de datos.

ANEXO 14

FLUJOGRAMA PARA LA GESTION DE ACUERDOS CON TERCEROS



ANEXO 15

ACUERDO DE CONFIDENCIALIDAD

COMPROMISO DE CONFIDENCIALIDAD DE LOS EMPLEADOS EN CUANTO AL USO Y DIVULGACIÓN DE INFORMACIÓN

Fecha: _____

Nombres y Apellidos: _____
DNI: _____ Área de Trabajo: _____

Cargo del Empleado: _____

En mi capacidad de empleado (ya sea tiempo parcial o tiempo completo) y en consideración de la relación laboral que mantengo con la organización / empresa, así como del acceso que se me permite a sus bases de información (Área de datos), constato que:

1. Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja mi empresa.

2. En concreto he leído, entiendo y me comprometo a cumplir los Procedimientos de Seguridad que corresponden a mi función en la empresa (descritos en la Política de Seguridad).

3. Me comprometo a cumplir, asimismo, todas las disposiciones relativas a la política de la empresa en materia de uso y divulgación de información, y a no divulgar la información que reciba a lo largo de mi relación con la empresa, subsistiendo este deber de secreto, aun después de que finalice dicha relación y tanto si esta información es de su propiedad, como si pertenece a un cliente de la misma, o a alguna otra organización que nos proporcione el acceso a dicha información, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.

4. Entiendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empresa y la posible reclamación por parte de la misma de los daños económicos causados.

_____

Firma Empleado/a

ANEXO 16

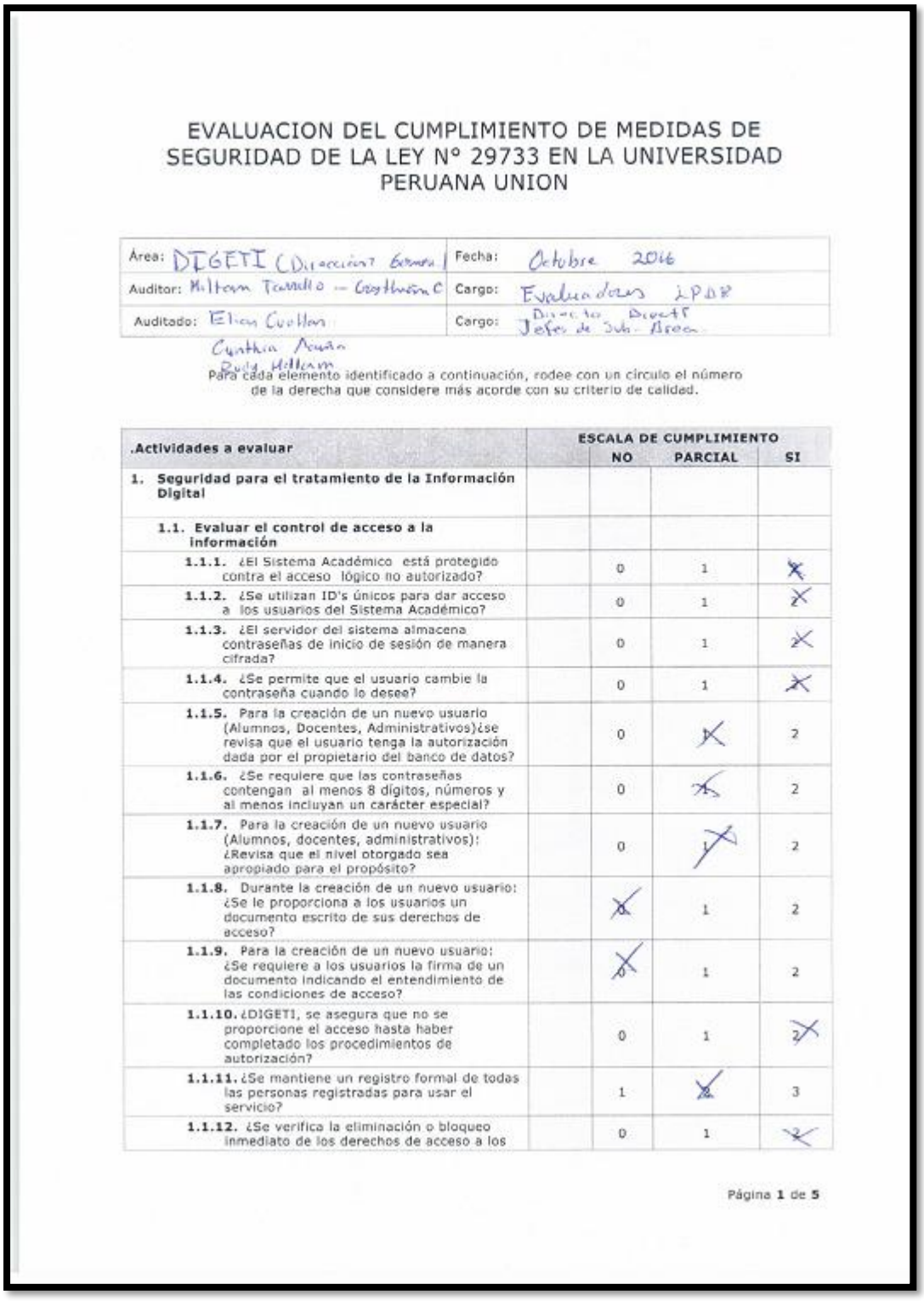
REGISTRO DE CONTROL DE DOCUMENTOS A DESTRUIR

Registro de control de documentos a destruir		
Empresa: Universidad Peruana Unión	**Aprobado por:** Secretario General	**Fecha:** 01/05/2017
Área: Secretaría General	**Elaborado por:** Equipo Investigador	**Versión:** 1.0

Nº	Código del documento (TUPA, Expediente u otros)	Nº de documentos	Nombre o Titulo del documento	Motivo de destrucción	Fecha	Responsable de destrucción	Responsable del documento	Estado	Observación
1	TUPA-0005-FRT34	10	Cambio de Director de Escuela	Documento dañado	10/05/2017	Aldous Huxley	Eliseo Fausto	Retirado	El documento esta dañado pero sirve aún para evidencia
2	Exp-003-56323	1	Carta de invitación a una reunión	Documento obsoleto	11/05/2017	Maria Campos	Maria Campos	Destruido	Ninguna

Importante: Al iniciar el procedimiento de destrucción de documentos será necesario consultar al Responsable del documento recibiendo el "visto bueno", evitando incidentes.

Anexo 11. Lista de chequeo del análisis GAP en DIGETI



EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

Área: DIGETI (Dirección Gener		Fecha:	Octubre 2016
Auditor: Milton Tarrillo – Cynthia C		Cargo:	Evaluadores LPDP
Auditado: Elias Cuellar		Cargo:	Director Digeti / Jefes de Sub. Area

Cynthia Acuña
Rudy Milton

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

.Actividades a evaluar		ESCALA DE CUMPLIMIENTO		
		NO	PARCIAL	SI
1. Seguridad para el tratamiento de la Información Digital				
1.1. Evaluar el control de acceso a la información				
1.1.1. ¿El Sistema Académico está protegido contra el acceso lógico no autorizado?		0	1	2
1.1.2. ¿Se utilizan ID's únicos para dar acceso a los usuarios del Sistema Académico?		0	1	2
1.1.3. ¿El servidor del sistema almacena contraseñas de inicio de sesión de manera cifrada?		0	1	2
1.1.4. ¿Se permite que el usuario cambie la contraseña cuando lo desee?		0	1	2
1.1.5. Para la creación de un nuevo usuario (Alumnos, Docentes, Administrativos)¿se revisa que el usuario tenga la autorización dada por el propietario del banco de datos?		0	1	2
1.1.6. ¿Se requiere que las contraseñas contengan al menos 8 dígitos, números y al menos incluyan un carácter especial?		0	1	2
1.1.7. Para la creación de un nuevo usuario (Alumnos, docentes, administrativos): ¿Revisa que el nivel otorgado sea apropiado para el propósito?		0	1	2
1.1.8. Durante la creación de un nuevo usuario: ¿Se le proporciona a los usuarios un documento escrito de sus derechos de acceso?		0	1	2
1.1.9. Para la creación de un nuevo usuario: ¿Se requiere a los usuarios la firma de un documento indicando el entendimiento de las condiciones de acceso?		0	1	2
1.1.10. ¿DIGETI, se asegura que no se proporcione el acceso hasta haber completado los procedimientos de autorización?		0	1	2
1.1.11. ¿Se mantiene un registro formal de todas las personas registradas para usar el servicio?		1	2	3
1.1.12. ¿Se verifica la eliminación o bloqueo inmediato de los derechos de acceso a los		0	1	2

Página **1** de **5**

usuarios que han cambiado de puesto o han dejado la organización?				
1.1.13. ¿Se asegura que no se emitan ID's redundantes a otros usuarios?		0	1	2
1.1.14. ¿Se realiza un chequeo periódico para eliminar o bloquear los ID's de usuario o cuentas redundantes?		0	1	2
1.2. Evaluar una correcta gestión de privilegios		**NO**	**PARCIAL**	**SI**
1.2.1. ¿Se cuentan con políticas donde se regule la disposición de privilegios al sistema?		0	1	2
1.2.2. ¿Se tiene un proceso de autorización debidamente documentado?		0	1	2
1.2.3. ¿Se otorga privilegios de acuerdo a la necesidad basándose las políticas de control de acceso?		0	1	2
1.2.4. ¿Se mantiene un registro de todos los privilegios asignados a los usuarios?		0	1	2
1.2.5. ¿Se verifica que no se otorguen privilegios hasta completar el proceso de autorización?		0	1	2
1.2.6. ¿Los privilegios se asignan a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio?		0	1	2
1.2.7. ¿Se revisan las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados?		0	1	2
1.2.8. ¿Se revisan las autorizaciones para los usuarios con privilegios especiales en intervalos de tiempo más cortos?		0	1	2
1.3. Evaluar los reportes de accesos		**NO**	**PARCIAL**	**SI**
1.3.1. ¿Se generan y mantienen registros que provean evidencia de accesos al sistema?		0	1	2
1.3.2. ¿Hay trazabilidad en los registros de acceso al sistema, como: horas de inicio, cierre de sesión y acciones relevantes?		0	1	2
1.4. Evaluar la realización del procedimiento documentado		**NO**	**PARCIAL**	**SI**
1.4.1. ¿Se cuenta con flujos de trabajos o procedimientos establecidos para el control de accesos?		0	1	2
1.4.2. ¿Se realizan las actividades de acuerdo a los procedimientos documentados?		0	1	2
1.4.3. ¿Se realizan auditorias de cumplimiento del control de accesos establecidos en la directiva de seguridad de la información de banco de datos personales?		0	1	2

Actividades a evaluar		ESCALA DE CUMPLIMIENTO		
	Peso:	NO	PARCIAL	SI
2. Conservación, respaldo y recuperación de Datos Personales				
2.1 Evaluar el control de seguridad en los ambientes que contienen datos				
2.1.1 ¿Los perímetros del edificio o local que contienen los medios de almacenamiento de Información son físicamente solidos?		0	1	2
2.1.2 ¿Las puertas y ventanas están protegidas de accesos no autorizados por mecanismos de control: Por ejemplo vallas, alarmas , relojes, etc.		0	1	2
2.1.3 ¿Los medios de almacenamiento de Información se encuentran físicamente separados de aquellos ajenos a la organización?		0	1	2
2.1.4 ¿Se usan controles de autenticación para restringir el acceso a los ambientes de procesamiento y almacenamiento de Información personal?		0	1	2
2.1.5 EL personal de servicios de ajenos al área ¿cuenta con acceso restringido a las áreas seguras o los medios de procesamiento de Información Personal?		0	1	2
2.2 Evaluar los Mecanismos de respaldo de la información		**NO**	**PARCIAL**	**SI**
2.2.1 ¿Se mantienen copias de seguridad del banco de datos personales?		0	1	2
2.2.2 ¿Las copias de respaldo de datos personales son protegidas mediante técnicas de cifrado?		0	1	2
2.2.3 ¿Las copias de respaldo se almacenan en un lugar físicamente apartado del local principal, para evitar algún daño por algún accidente o desastre natural?		0	1	2
2.2.4 La Información de respaldo cuenta con el mismo nivel de seguridad física y ambiental que el local principal.		0	1	2
2.2.5 ¿Los medios de respaldos se prueban regularmente para comprobar su correcto funcionamiento?		0	1	2
2.3 Evaluar procedimientos de restauración de respaldos.		**NO**	**PARCIAL**	**SI**
2.3.1 ¿Los procedimientos de restauración se chequean y prueban regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación?		0	1	2
2.3.2 ¿Las pruebas realizadas a los respaldos cuentan con la documentación adecuada?(fecha y hora de la prueba, nombre del que realizo, BDP recuperado, tiempo de recuperación, resultados de la pruebas)		0	1	2
2.3.3 ¿Se toman acciones en caso de pruebas insatisfactorias?		0	1	2

2.3.4 Cuando se restaura una copia de seguridad del banco de datos personales ¿se requiere autorización del titular de BDP o quien es te asignado?		0	1	2
Actividades a evaluar	**Peso:**	**ESCALA DE CUMPLIMIENTO** **NO**	**PARCIAL**	**SI**
3. Transferencia lógica o electrónica de Datos Personales.				
3.1. Supervisar la autorización del titular del BDP para la transferencia.				
3.1.1. Se cuentan con políticas para la transferencia lógica o electrónica de Datos Personales		0	1	2
3.1.2. ¿El tratamiento de datos personales es autorizado por el titular del banco de datos personales?		0	1	2
3.1.3. ¿Se cuenta con algún documento que garantice la trasferencia Internacional de Datos Personales?		0	1	2
3.1.4. ¿Se procede a la transferencia Datos Personales aun sin la autorización previa del Titular de Banco de Datos o encargado?		0	1	2
3.2. Medios de transporte para la transferencia de datos personales.		**NO**	**PARCIAL**	**SI**
3.2.1. ¿Se cuentan con medios de envío autorizados Titular de BDP para la trasferencia de Datos?		0	1	2
3.2.2. ¿Se controla el uso de los medios de transferencia de datos personales?		0	1	2
3.2.3. ¿Existe evidencia documentada del uso de los medios de transferencia establecidos?		0	1	2
3.2.4. ¿Se utilizan software especializado para la transferencia de datos personales?		0	1	2
3.3. **Mecanismos de Seguridad en la transferencia de Datos Personales**				
3.3.1. ¿Se encuentran establecidos los mecanismos de seguridad para la transferencia en las políticas?		0	1	2
3.3.2. ¿Los equipos utilizados para la transferencia lógica cuentan con software de protección contra códigos maliciosos?		0	1	2
3.3.3. ¿Se utilizan protocolos de comunicación cifrados como: VPN, correo electrónico cifrado, FTP seguro, otros?]		0	1	2
3.3.4. Los datos contenidos en soporte informático ¿se transportan previa encriptación y un mecanismo de verificación de la integridad?		0	1	2
3.3.5. El Área de tratamiento de datos personales tiene restringido el uso de herramientas de registro no autorizadas? (cámara de video , fotográficas, grabación de audio ,etc.)		0	1	2

4. Prestación de servicios sin acceso a datos personales				
4.1. Servicios internos de la organización o área sin acceso a datos personales				
4.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		0	X	2
4.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		0	1	X
4.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		X	1	2
4.1.4. ¿Se generan documentos mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		X	1	2
4.2. Servicios externos a la organización sin acceso a datos personales		**NO**	**PARCIAL**	**SI**
4.2.1. ¿Se generan contratos expresos o cláusulas contractuales sobre el tratamiento de datos personales al momento de prestar servicios externos?		0	X	2
4.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?		X	1	2
4.2.3. ¿Existe algún documento que garantice la destrucción o imposibilidad de recuperación de los datos alojados en el servicio del prestador de servicio una vez concluida la relación con el proveedor?		X	1	2
4.2.4. ¿Se realizan visitas a la infraestructura del proveedor para comprobar el cumplimiento del servicio? O en caso de un proveedor extranjero: ¿Los prestadores de servicio cuentan con reportes SOC para verificar el cumplimiento del servicio?		0	X	2
4.2.5.				

X
Auditor Externo

X
Encargado Área Auditada

X
Director de DIGETI

Página **5** de **5**

Anexo 12. Lista de chequeo del análisis GAP en Secretaría General

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIONIU

Área: Secretaría General	Fecha: 28/09
Auditor: Milton Torrillo	Cargo: Auditor
Auditado: Paul Huaman	Cargo: Encargado de TI

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

PAUL

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada			
1.1. Almacenamiento de documentación no automatizada			
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.	0	1	2 X
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?	0	1	2 X
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?	0	1 X	2
1.2. Copia o reproducción de la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?	0	1 X	2 X
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? 1.2.2.1.1. Sin permitir su recuperación.	0	1 X	2
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?	0	1	2 X
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos	0	1	2 X
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?	0	1	2 X
1.3. Acceso a la documentación no automatizada	0	1	2

Página **1** de **4**

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIONIU

1.3.1. ¿Se cuenta con algún documento donde indique la responsabilidad que recae en el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos personales?		0	1	2
1.3.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?		0	1	2
1.3.3. ¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?		0	1	2
1.3.4. ¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?		0	1	2

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	**ESCALA DE CUMPLIMIENTO**			
	Peso:	**NO**	**PARCIAL**	**SI**
2. Traslado de la documentación no automatizada				
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado				
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?		0	1	2
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?		0	1	2
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?		0	1	2
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?		0	1	2
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?		0	1	2
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?		0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIONIU

2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.		0	1	2
2.2. **Eventos o incidentes en el traslado de datos personales**				
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?		0	1	2
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?		0	1	2
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?		0	1	2

Actividades a evaluar	ESCALA DE CUMPLIMIENTO			
	Peso:	NO	PARCIAL	SI
3. Prestación de servicios sin acceso a datos personales	**20%**			
3.1. **Servicios internos de la organización o área sin acceso a datos personales**	**10%**			
3.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		0	1	2
3.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		0	1	2
3.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		NA	NA 1	NA 2
3.1.4. ¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIONIU

2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.	0	1	2
2.2. **Eventos o incidentes en el traslado de datos personales**			
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?	0	1	2
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?	0	1	2
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?	0	1	2

Actividades a evaluar	ESCALA DE CUMPLIMIENTO			
	Peso:	NO	PARCIAL	SI
3. Prestación de servicios sin acceso a datos personales	**20%**			
3.1. **Servicios internos de la organización o área sin acceso a datos personales**	**10%**			
3.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		0	1	2
3.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		0	1	2
3.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		NA	NA 1	NA 2
3.1.4. ¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIONIU

3.2.	**Servicios externos a la organización sin acceso a datos personales**	**10%**	**NO**	**PARCIAL**	**SI**
3.2.1.	¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?		0	1	2
3.2.2.	¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?		0	1	2
3.2.3.	¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?		0	1	2
3.2.4.	¿Existe algún documento que garantice la destrucción o imposibilidad de recuperación de los datos alojados en el servicio del prestador de servicio una vez concluida la relación con el proveedor?		0	1	2
3.2.5.	¿Se realizan visitas a la infraestructura del proveedor para comprobar el cumplimiento del servicio? O en caso de un proveedor extranjero: ¿Los prestadores de servicio cuentan con reportes SOC para verificar el cumplimiento del servicio?		0	1	2

X _____
Auditor Externo

X _____
Encargado Área Auditada

X _____
Director de DIGETI

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

Área:	Secretaría General	Fecha:	28/09
Auditor:	Hilton Tonillo	Cargo:	Auditor
Auditado:	Noelia Melendez	Cargo:	Encargado de oficina

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada			
1.1. Almacenamiento de documentación no automatizada			
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.	0	1	2
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?	0	1	2
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?	0	1	2
1.2. Copia o reproducción de la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?	0	1	2
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? ¿Sin permitir su recuperación?	0	1	2
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?	0	1	2
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos	0	1	2
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?	0	1	2
1.3. Acceso a la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.3.1. ¿Se cuenta con algún documento donde indique la responsabilidad que recae en el titular del banco de dato o el responsable ante algún incidente	0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY Nº 29733 EN LA UNIVERSIDAD PERUANA UNION

relacionado al acceso no autorizado de los documentos que contengan datos personales?				
1.3.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?		0	1	2
1.3.3. ¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?		0	1	2
1.3.4. ¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?		0	1	2

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
2. Traslado de la documentación no automatizada			
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado			
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?	0	1	2
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?	0	1	2
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?	0	1	2
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?	0	1	2
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?	0	1	2
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?	0	1	2
2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.	0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

		NO	PARCIAL	SI
2.2. **Eventos o incidentes en el traslado de datos personales**				
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?		0	1	2
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?		0	1	2
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?		0	1	2

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar		ESCALA DE CUMPLIMIENTO		
		NO	PARCIAL	SI
3. Prestación de servicios sin acceso a datos personales				
3.1. **Servicios internos de la organización o área sin acceso a datos personales**				
3.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		0	1	2
3.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		0	1	2
3.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		0	1	2
3.1.4. ¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		0	1	2
3.2. **Servicios externos a la organización sin acceso a datos personales**		NO	PARCIAL	SI
3.2.1. ¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?		0	1	2
3.2.2. ¿Se generan contratos de obligación de secreto (compromiso de		0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY Nº 29733 EN LA UNIVERSIDAD PERUANA UNION

	confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?	X			
3.2.3.	¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?	X	0	1	2

X _____
Auditor Externo

X _____
Encargado Área Auditada

X _____
Secretario General

Página **4** de **4**

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

Área: Secretaria General	Fecha: 28/09
Auditor: Nilton Torrillo	Cargo: Auditor
Auditado: Herminia	Cargo: Encargada de Filial de Ingreso

Herminia → Guarda y almacena y autoriza (Filial de ingreso).

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada			
1.1. Almacenamiento de documentación no automatizada			
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.	0	1	2
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?	0	1	2
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?	0	1	2
1.2. Copia o reproducción de la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?	0	1	2
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? ¿Sin permitir su recuperación?	0	1	2
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?	0	1	2
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos	0	1	2
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?	0	1	2
1.3. Acceso a la documentación no automatizada	**NO**	**PARCIAL**	**SI**
1.3.1. ¿Se cuenta con algún documento donde indique la responsabilidad que recae en el titular del banco de dato o el responsable ante algún incidente	0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

relacionado al acceso no autorizado de los documentos que contengan datos personales?				
1.3.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?		0	1	2
1.3.3. ¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?		0	1	2
1.3.4. ¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?		0	1	2

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
2. Traslado de la documentación no automatizada			
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado			
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?	0	1	2
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?	0	1	2
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?	0	1	2
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?	0	1	2
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?	0	1	2
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?	0	1	2
2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.	0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY Nº 29733 EN LA UNIVERSIDAD PERUANA UNION

		NO	PARCIAL	SI
2.2. **Eventos o incidentes en el traslado de datos personales**				
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?		0	1	2
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos personales es notificado inmediatamente al titular de los datos personales?		0	1	2
2.2.3. ¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?		0	1	2

Para cada elemento identificado a continuación, rodee con un circulo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO		
	NO	PARCIAL	SI
3. Prestación de servicios sin acceso a datos personales			
3.1. **Servicios internos de la organización o área sin acceso a datos personales**			
3.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?	0	1	2
3.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?	0	1	2
3.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.	0	1	2
3.1.4. ¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?	0	1	2
3.2. **Servicios externos a la organización sin acceso a datos personales**	**NO**	**PARCIAL**	**SI**
3.2.1. ¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?	0	1	2
3.2.2. ¿Se generan contratos de obligación de secreto (compromiso de	0	1	2

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

	confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?	X			
3.2.3.	¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?	X	0	1	2

X
Auditor Externo

X
Encargado Área Auditada

X
Secretario General

Anexo 13. Actas de reuniones con el personal de Secretaría General

UNIVERSIDAD PERUANA UNIÓN

Implementación de controles de Seguridad para el cumplimento de la Ley 29733

Una Institución Adventista

ACTA DE REUNIÓN

Lugar	Oficina Secretaria General	Horario			
Fecha	Miércoles 24 de Mayo del 2016	**H. Inicio**	2.:20	**H. término**	3:00

2:40 4:50

Agenda:	
1	Implementación de controles de seguridad para el cumplimiento de la Ley Nro 29733 en Secretaria General

Miembros	
Expositor	Bach. Milton Tarrillo Villegas
Expositor	Bach. Cristhian Calisaya Sana

ASISTENTES

	Miembros	Cargo	Firma
1	Mg. Edgar Horna Santillán	Secretario General Upeu	
2	Marilu Malandaz S.	Secretaña	
3	Maria Cueva Cueva	Secretaria	
4	Miriam Torres Lozano	Secretaria	
5	Susana Dávila	Secretaria	
6	Emily Siu Gonzales	Secretaria	
7	Yenny Mamani Rodrigo	Secretaria.	
8	Steve Shica Sivipaucar	Jefe de Grados y Titulos	
9	Salomé Vallejos R	Trámite Documentario	
10	Andi Huamacto Conde	Tramites Documentario	
11	Jack Castillo Ramos	Estadistica e información	

12	Raul Huaman Vivas	Estadística e Información	
13	Wilberth Gonzales Feco		
14	Ruth Tavita Ocostegui Melendrez	Registro Academico	
15	Dany Millones Lizo	Registro Académico	

UNIVERSIDAD PERUANA UNIÓN

Una Institución Adventista

ACTA DE REUNIÓN

2da Reunión de Concientización en Protección de Datos Personales.

Lugar	Secretaria General
Fecha	Jueves 17 de agosto de 2017

Horario			
H. Inicio	8:00 am	H. término	8:30 am

Agenda:	
1	Capacitación para el llenado de documentos requeridos en las propuestas de protección de datos personales.

Miembros	
Capacitador.	Bach. Milton Tarrillo
Capacitador.	Bach. Cristhian Calisaya

ASISTENTES

	Miembros	Cargo	Area	Firma
1	Mariluz Malendaz Salazar	Secretaria	Reg. Administ.	
2	Steve Shica Sivipaucar	Jefe de Grados y Títulos	Grados y títulos	
3	Dany Y. Milloness Lizc.	Registro Académico	Reg. Acad.	
4	Ruth T Anostegui Melendrez	Registro Académico	Reg. Acad	
5	Yenny Mamani Rodrigz	Proceso de Grados.	Grados y títul	
6	Salomé Vallejos Roque	Trámite Docum.	Secretaria	
7	Milagros M Conca Afoca[illegible]	Secretaria	Trám. Doc	
8	Emily T. Siu Gonzales	Secretaria	Grados y Títulos	
9	Jack C. Castillo Ramos	Asistente	Estadística	
10	Paul A Huaman Vivas	T I	Estadística	

11	Yamis Jorge Merma	Secretario	Reg. Administrativo	
12				
13				
14				
15				

Anexo 14. Lista de chequeo de la evaluación final en Secretaría General

EVALUACIÓN DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

Área: Secretaria General	Fecha: 22/01/2018
Evaluador: Milton Torrillo Villca	Cargo: Evaluador I
Trabajador: Moiles Melendez	Cargo: Secretaria - Registro Adm.

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	ESCALA DE CUMPLIMIENTO			
	Peso:	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada				
1.1. Almacenamiento de documentación no automatizada				
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.		NA		
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?		NA		
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?		NA		
1.2. Copia o reproducción de la documentación no automatizada				
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?				X
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? Sin permitir su recuperación.				X
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?				X
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos				X
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?				X
1.3. Acceso a la documentación no automatizada				
1.3.1 ¿Se cuenta con algún documento donde indique la responsabilidad que recae en				

Página **1** de **3**

	el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos personales?		X		
1.3.2	¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?				X
1.3.3	¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?				X
1.3.4	¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?				X

Actividades a evaluar		ESCALA DE CUMPLIMIENTO			
		Peso:	NO	PARCIAL	SI
2.	**Traslado de la documentación no automatizada**				
2.1.	**Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado**				
2.1.1.	¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?				X
2.1.2.	¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?				X
2.1.3.	¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?				X
2.1.4.	¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?				X
2.1.5.	¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?			X	
2.1.6.	¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?		X		
2.1.7.	¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.		X		
2.2.	**Eventos o incidentes en el traslado de datos personales**				
2.2.1.	¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?				X
2.2.2.	¿Todo evento o incidente con algún documento que contenga datos				

	personales es notificado inmediatamente al titular de los datos personales?				X
2.2.3.	¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?				X

Actividades a evaluar		ESCALA DE CUMPLIMIENTO			
		Peso:	NO	PARCIAL	SI
3. Prestación de servicios sin acceso a datos personales					
3.1. Servicios internos de la organización o área sin acceso a datos personales					
3.1.1.	¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		NA		
3.1.2.	¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		NA		
3.1.3.	¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		NA		
3.1.4.	¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		NA		
3.2.	**Servicios externos a la organización sin acceso a datos personales**				
3.2.1.	¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?		NA		
3.2.2.	¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?				X
3.2.3.	¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?		NA		

X
Auditor Externo

X
Encargado Área Auditada

X
Secretario General

EVALUACIÓN DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

Área: Secretaria General.	Fecha: 23 /01 /18
Auditor: Cristhian Calcuya Sana	Cargo: Evaluador II
Auditado: Danny Milmer	Cargo: Sec. Registro Académico

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	Peso:	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada	**50%**			
1.1. Almacenamiento de documentación no automatizada	**40%**			
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.		1	2	X
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?		1	2	X
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?		1	2	X
1.2. Copia o reproducción de la documentación no automatizada	**30%**	**NO**	**PARCIAL**	**SI**
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?		1	2	X
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? Sin permitir su recuperación.				X
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?		1	X	3
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos				X
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?				X
1.3. Acceso a la documentación no automatizada	**30%**	1	2	3
1.3.1 ¿Se cuenta con algún documento donde indique la responsabilidad que recae en				X

	el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos personales?				X
1.3.2	¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?		1	2	X
1.3.3	¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?		1	2	X
1.3.4	¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?		1	2	X

Actividades a evaluar		ESCALA DE CUMPLIMIENTO			
		Peso:	NO	PARCIAL	SI
2.	**Traslado de la documentación no automatizada**	**30%**			
2.1.	**Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado**	**55%**			
2.1.1.	¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?				X
2.1.2.	¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?		1	X	3
2.1.3.	¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?		1	2	X
2.1.4.	¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?		1	2	X
2.1.5.	¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?		X		
2.1.6.	¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?		X	2	3
2.1.7.	¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.		X		
2.2.	**Eventos o incidentes en el traslado de datos personales**	**45%**			
2.2.1.	¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?		1	2	X
2.2.2.	¿Todo evento o incidente con algún documento que contenga datos		1	2	3

	personales es notificado inmediatamente al titular de los datos personales?			X
2.2.3.	¿Todo evento o acción relacionada al acceso o manipulación de algún documento que contenga datos personales es reportado inmediatamente a la gerencia?			X

Actividades a evaluar		ESCALA DE CUMPLIMIENTO			
		Peso:	NO	PARCIAL	SI
3.	**Prestación de servicios sin acceso a datos personales**	**20%**			
3.1.	**Servicios internos de la organización o área sin acceso a datos personales**	**50%**			
3.1.1.	¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		NA 1	2	3
3.1.2.	¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		NA 1	2	3
3.1.3.	¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		NA 1	2	3
3.1.4.	¿Se generan documentos por escrito mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		NA 1	2	3
3.2.	**Servicios externos a la organización sin acceso a datos personales**	**50%**	**NO**	**PARCIAL**	**SI**
3.2.1.	¿Se generan contratos expresos o cláusulas contractuales a detalle sobre el tratamiento de datos personales al momento de prestar servicios externos?		NA 1	2	3
3.2.2.	¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?		NA 1	2	X
3.2.3.	¿Existe algún documento que respalde que el prestador de servicios externo no brinde acceso a terceros de los datos personales que utilice?		NA 1	2	3

X
Auditor Externo

X
Encargado Área Auditada

X
Secretario General

EVALUACIÓN DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNIÓN

Área: Secretaria General	Fecha: 24/01/2018
Auditor: Milton Tonillo Villegas	Cargo: Auditor I
Auditado: Martha Rosco Plasencia	Cargo: Secretaria de Archivo

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

Actividades a evaluar	Peso:	NO	PARCIAL	SI
1. Almacenamiento, copia y acceso a la documentación no automatizada	**50%**			
1.1. Almacenamiento de documentación no automatizada	**40%**			
1.1.1. ¿Los archivadores de datos personales se encuentran en áreas con acceso protegido? Ejemplo: Llave, cerradura, dispositivos u otros.		1	2	3
1.1.2. ¿Las áreas donde se encuentren documentos que contiene datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos?		1	2	3
1.1.3. ¿Los documentos que contiene datos personales se almacenan independientemente de modo que no pueda exponerse otra información?		1	2	3
1.2. Copia o reproducción de la documentación no automatizada	**30%**	**NO**	**PARCIAL**	**SI**
1.2.1. ¿El titular del banco de datos o el responsable, designa a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales?		1	2	3
1.2.2. ¿Se procede a la destrucción completa de las copias o reproducciones desechas de los datos personales? Sin permitir su recuperación.				
1.2.3. ¿Se utiliza impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados?		1	2	3
1.2.4. ¿Se supervisa el proceso de copia o reproducción de los documentos? No dejando desatendido los equipos				
1.2.5. ¿Se retiran los documentos originales y las copias inmediatamente del equipo habiendo finalizado el proceso de copia o reproducción?				
1.3. Acceso a la documentación no automatizada	**30%**	1	2	3
1.3.1 ¿Se cuenta con algún documento donde indique la responsabilidad que recae en				

	el titular del banco de dato o el responsable ante algún incidente relacionado al acceso no autorizado de los documentos que contengan datos personales?				
1.3.2	¿El titular del banco de datos, o el encargado autoriza o retira el acceso de usuarios a los datos personales?		1	2	3
1.3.3	¿Se encuentra registrado una lista de los usuarios autorizados o no a los datos personales?		1	2	3
1.3.4	¿Se tiene un registro (persona, fecha, hora, motivo) de los accesos a los datos personales?		1	2	3

Actividades a evaluar		ESCALA DE CUMPLIMIENTO		
	Peso:	NO	PARCIAL	SI
2. Traslado de la documentación no automatizada	**30%**			
2.1. Medidas para impedir el acceso o manipulación a los datos personales objeto de traslado	**55%**			
2.1.1. ¿Las operaciones de traslado de documentos que contengan datos personales se da solo con la autorización del titular del banco de datos o el responsable?				
2.1.2. ¿El titular del banco de datos, o el encargado autoriza o retira el acceso a usuarios o mensajeros para que trasladen documentos que contengan datos personales?		1	2	3
2.1.3. ¿Se encuentra registrado una lista de los usuarios o mensajeros autorizados o no a trasladar documentos que contengan datos personales?		1	2	3
2.1.4. ¿Se tiene un registro (persona y/o empresa, fecha, hora, motivo) de los usuarios o mensajeros autorizados a trasladar documentos que contengan datos personales?		1	2	3
2.1.5. ¿El contenedor, sobre o archivador evita el fácil acceso y legibilidad de los datos personales?				
2.1.6. ¿Se cuenta con algún mecanismo de verificación de no vulneración al contenedor?		1	2	3
2.1.7. ¿La información sensible cuenta con controles especiales para proteger la información? Ejemplo: Envase con detección de apertura, entrega en mano, varias entregas por rutas distintas.				
2.2. Eventos o incidentes en el traslado de datos personales	**45%**			
2.2.1. ¿Se registran los incidentes de seguridad relacionado al acceso o manipulación en el traslado de documentos que contengan datos personales?		1	2	3
2.2.2. ¿Todo evento o incidente con algún documento que contenga datos		1	2	3

Anexo 15. Lista de chequeo de la evaluación final en DIGETI

EVALUACION DEL CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD DE LA LEY N° 29733 EN LA UNIVERSIDAD PERUANA UNION

Área: Direccion General de Tecnologias I.	Fecha: 8 de Octubre de 2018.
Auditor: Gaothian Calsaya - Milton Tamb	Cargo: Investigador
Auditado: Rocio Tapia - Denis Urquizo.	Cargo: Jefes de Area.

Para cada elemento identificado a continuación, rodee con un círculo el número de la derecha que considere más acorde con su criterio de calidad.

.Actividades a evaluar	ESCALA DE CUMPLIMIENTO NO	PARCIAL	SI
1. Seguridad para el tratamiento de la Información Digital			
1.1. Evaluar el control de acceso a la información			
1.1.1. ¿El Sistema Académico está protegido contra el acceso lógico no autorizado?	0	1	2
1.1.2. ¿Se utilizan ID's únicos para dar acceso a los usuarios del Sistema Académico?	0	1	2
1.1.3. ¿El servidor del sistema almacena contraseñas de inicio de sesión de manera cifrada?	0	1	2
1.1.4. ¿Se permite que el usuario cambie la contraseña cuando lo desee?	0	1	2
1.1.5. Para la creación de un nuevo usuario (Alumnos, Docentes, Administrativos)¿se revisa que el usuario tenga la autorización dada por el propietario del banco de datos?	0	1	2
1.1.6. ¿Se requiere que las contraseñas contengan al menos 8 dígitos, números y al menos incluyan un carácter especial?	0	1	2
1.1.7. Para la creación de un nuevo usuario (Alumnos, docentes, administrativos): ¿Revisa que el nivel otorgado sea apropiado para el propósito?	0	1	2
1.1.8. Durante la creación de un nuevo usuario: ¿Se le proporciona a los usuarios un documento escrito de sus derechos de acceso?	0	1	2
1.1.9. Para la creación de un nuevo usuario: ¿Se requiere a los usuarios la firma de un documento indicando el entendimiento de las condiciones de acceso?	0	1	2
1.1.10. ¿DIGETI, se asegura que no se proporcione el acceso hasta haber completado los procedimientos de autorización?	0	1	2
1.1.11. ¿Se mantiene un registro formal de todas las personas registradas para usar el servicio?	1	2	3
1.1.12. ¿Se verifica la eliminación o bloqueo inmediato de los derechos de acceso a los	0	1	2

Página **1** de **5**

usuarios que han cambiado de puesto o han dejado la organización?				
1.1.13. ¿Se asegura que no se emitan ID's redundantes a otros usuarios?		0	1	2
1.1.14. ¿Se realiza un chequeo periódico para eliminar o bloquear los ID's de usuario o cuentas redundantes?		0	1	2
1.2. Evaluar una correcta gestión de privilegios		**NO**	**PARCIAL**	**SI**
1.2.1. ¿Se cuentan con políticas donde se regule la disposición de privilegios al sistema?		0	1	2
1.2.2. ¿Se tiene un proceso de autorización debidamente documentado?		0	1	2
1.2.3. ¿Se otorga privilegios de acuerdo a la necesidad basándose las políticas de control de acceso?		0	1	2
1.2.4. ¿Se mantiene un registro de todos los privilegios asignados a los usuarios?		0	1	2
1.2.5. ¿Se verifica que no se otorguen privilegios hasta completar el proceso de autorización?		0	1	2
1.2.6. ¿Los privilegios se asignan a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio?	N/A	0	1	2
1.2.7. ¿Se revisan las asignaciones de privilegios a intervalos regulares para asegurar que no se obtengan privilegios no autorizados?		0	1	2
1.2.8. ¿Se revisan las autorizaciones para los usuarios con privilegios especiales en intervalos de tiempo más cortos?		0	1	2
1.3. Evaluar los reportes de accesos		**NO**	**PARCIAL**	**SI**
1.3.1. ¿Se generan y mantienen registros que provean evidencia de accesos al sistema?		0	1	2
1.3.2. ¿Hay trazabilidad en los registros de acceso al sistema, como: horas de inicio, cierre de sesión y acciones relevantes?		0	1	2
1.4. Evaluar la realización del procedimiento documentado		**NO**	**PARCIAL**	**SI**
1.4.1. ¿Se cuenta con flujos de trabajos o procedimientos establecidos para el control de accesos?		0	1	2
1.4.2. ¿Se realizan las actividades de acuerdo a los procedimientos documentados?		0	1	2
1.4.3. ¿Se realizan auditorias de cumplimiento del control de accesos establecidos en la directiva de seguridad de la información de banco de datos personales?		0	1	2

Actividades a evaluar		ESCALA DE CUMPLIMIENTO		
	Peso:	NO	PARCIAL	SI
2. Conservación, respaldo y recuperación de Datos Personales				
2.1 Evaluar el control de seguridad en los ambientes que contienen datos				
2.1.1 ¿Los perímetros del edificio o local que contienen los medios de almacenamiento de Información son físicamente solidos?		0	1	2
2.1.2 ¿Las puertas y ventanas están protegidas de accesos no autorizados por mecanismos de control: Por ejemplo vallas, alarmas , relojes, etc.		0	1	2
2.1.3 ¿Los medios de almacenamiento de Información se encuentran físicamente separados de aquellos ajenos a la organización?		0	1	2
2.1.4 ¿Se usan controles de autenticación para restringir el acceso a los ambientes de procesamiento y almacenamiento de Información personal?		0	1	2
2.1.5 EL personal de servicios de ajenos al área ¿cuenta con acceso restringido a las áreas seguras o los medios de procesamiento de Información Personal?		0	1	2
2.2 Evaluar los Mecanismos de respaldo de la información		**NO**	**PARCIAL**	**SI**
2.2.1 ¿Se mantienen copias de seguridad del banco de datos personales?		0	1	2
2.2.2 ¿Las copias de respaldo de datos personales son protegidas mediante técnicas de cifrado?		0	1	2
2.2.3 ¿Las copias de respaldo se almacenan en un lugar físicamente apartado del local principal, para evitar algún daño por algún accidente o desastre natural?		0	1	2
2.2.4 La Información de respaldo cuenta con el mismo nivel de seguridad física y ambiental que el local principal.		0	1	2
2.2.5 ¿Los medios de respaldos se prueban regularmente para comprobar su correcto funcionamiento?		0	1	2
2.3 Evaluar procedimientos de restauración de respaldos.		**NO**	**PARCIAL**	**SI**
2.3.1 ¿Los procedimientos de restauración se chequean y prueban regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación?		0	1	2
2.3.2 ¿Las pruebas realizadas a los respaldos cuentan con la documentación adecuada?(fecha y hora de la prueba, nombre del que realizo, BDP recuperado, tiempo de recuperación, resultados de la pruebas)		0	1	2
2.3.3 ¿Se toman acciones en caso de pruebas insatisfactorias?		0	1	2

2.3.4 Cuando se restaura una copia de seguridad del banco de datos personales ¿se requiere autorización del titular de BDP o quien es te asignado?		0	1	2
Actividades a evaluar	**Peso:**	**ESCALA DE CUMPLIMIENTO** NO	PARCIAL	SI
3. Transferencia lógica o electrónica de Datos Personales.				
3.1. Supervisar la autorización del titular del BDP para la transferencia.				
3.1.1. Se cuentan con políticas para la transferencia lógica o electrónica de Datos Personales		0	1	2
3.1.2. ¿El tratamiento de datos personales es autorizado por el titular del banco de datos personales?		0	1	2
3.1.3. ¿Se cuenta con algún documento que garantice la trasferencia Internacional de Datos Personales?		0	1	2
3.1.4. ¿Se procede a la transferencia Datos Personales aun sin la autorización previa del Titular de Banco de Datos o encargado?		0	1	2
3.2. Medios de transporte para la transferencia de datos personales.		**NO**	**PARCIAL**	**SI**
3.2.1. ¿Se cuentan con medios de envío autorizados Titular de BDP para la trasferencia de Datos?		0	1	2
3.2.2. ¿Se controla el uso de los medios de transferencia de datos personales?		0	1	2
3.2.3. ¿Existe evidencia documentada del uso de los medios de transferencia establecidos?		0	1	2
3.2.4. ¿Se utilizan software especializado para la transferencia de datos personales?		0	1	2
3.3. **Mecanismos de Seguridad en la transferencia de Datos Personales**				
3.3.1. ¿Se encuentran establecidos los mecanismos de seguridad para la transferencia en las políticas?		0	1	2
3.3.2. ¿Los equipos utilizados para la transferencia lógica cuentan con software de protección contra códigos maliciosos?		0	1	2
3.3.3. ¿Se utilizan protocolos de comunicación cifrados como: VPN, correo electrónico cifrado, FTP seguro, otros?|		0	1	2
3.3.4. Los datos contenidos en soporte informático ¿se transportan previa encriptación y un mecanismo de verificación de la integridad?		0	1	2
3.3.5. El Área de tratamiento de datos personales tiene restringido el uso de herramientas de registro no autorizadas? (cámara de video , fotográficas, grabación de audio ,etc.)		0	1	2

4. Prestación de servicios sin acceso a datos personales				
4.1. Servicios internos de la organización o área sin acceso a datos personales				
4.1.1. ¿El responsable o el encargado del tratamiento limita el acceso del personal a los documentos que contengan datos personales?		0	1	2
4.1.2. ¿El responsable o el encargado del tratamiento limita la realización de trabajos que no impliquen el tratamiento de datos personales?		0	1	2
4.1.3. ¿Se restringe el uso de equipos de fotografía, video, audio u otra forma de registro en el área de tratamiento de datos personales? Salvo autorización del titular del banco de datos personales o el encargado.		0	1	2
4.1.4. ¿Se generan documentos mediante cláusulas contractuales los límites y el detalle de la prestación de servicios internos?		0	1	2
4.2. Servicios externos a la organización sin acceso a datos personales		**NO**	**PARCIAL**	**SI**
4.2.1. ¿Se generan contratos expresos o cláusulas contractuales sobre el tratamiento de datos personales al momento de prestar servicios externos?		0	1	2
4.2.2. ¿Se generan contratos de obligación de secreto (compromiso de confidencialidad) respecto a los datos que el personal externo hubiera podido conocer por motivo de prestación de servicio?		0	1	2
4.2.3. ¿Existe algún documento que garantice la destrucción o imposibilidad de recuperación de los datos alojados en el servicio del prestador de servicio una vez concluida la relación con el proveedor?		0	1	2
4.2.4. ¿Se realizan visitas a la infraestructura del proveedor para comprobar el cumplimiento del servicio? O en caso de un proveedor extranjero: ¿Los prestadores de servicio cuentan con reportes SOC para verificar el cumplimiento del servicio?	N/P	0	1	2
4.2.5.				

X

Auditor Externo

X

Encargado Área Auditada

X

Director de DIGETI